



# ***Risk Management (P3)***

Spread the word about OpenTuition, so that all CIMA students can benefit.

#### How to use OpenTuition:

- 1) Register & download the latest notes
- 2) Watch ALL OpenTuition free lectures
- 3) Attempt free tests online
- 4) **Question practice is vital** - you must obtain also Exam Kit from Kaplan or BPP



**AICPA® & CIMA®**

Registered Tuition Provider



**The best things  
in life are free**

## **IMPORTANT!!! PLEASE READ CAREFULLY**

To benefit from these notes you **must** watch the free lectures on the OpenTuition website in which we explain and expand on the topics covered.

In addition question practice is vital!!

You **must** obtain a current edition of a Revision / Exam Kit - the CIMA approved publisher is Kaplan. It contains a great number of exam standard questions (and answers) to practice on.

We also recommend getting extra questions from BPP - if you order on line, you can use our 20% discount code: **bppcima20optu**

You should also use our free “Practice Tests” and flashcards which you can find on the OpenTuition website:

**<https://opentuition.com/cima/>**

# CIMA P3

## Risk Management

	Overview of Paper P3	3
1.	The types of risk facing an organisation	5
2.	Responses to risk	11
3.	Enterprise risk management	23
4.	Some quantitative techniques	31
5.	Corporate governance	43
6.	Internal control and auditing	49
7.	Ethical considerations	65
8.	Cyber risks	69





## OVERVIEW OF PAPER P3

The syllabus consists of the following sections

A	Enterprise risk	This looks at the types of risk that organisations are subject to, how those risks can be assessed and how the risks can be dealt with.
B	Strategic risk	Strategic risk relates to long term risk: wrong products, wrong market location, effects of technology and other long term changes.
C	Internal controls	Internal controls enable organisations to be managed and directed in a coherent way. Transactions are properly recorded, assets are safeguarded and information used by management is accurate. The operation of internal controls can be investigated by internal audit.
D	Cyber risks	With more and more reliance on IT for both recording transactions and as the mechanism by which value is delivered to shareholders, it is imperative that cyber risks (ie risks relating to IT) are properly addressed.





# Chapter 1

## THE TYPES OF RISK FACING AN ORGANISATION

### 1. What is risk?

'Risk is a condition in which there exists a quantifiable dispersion in the possible outcomes from any activity. It can be classified in a number of ways.'

CIMA Official Terminology, 2005

The key word in this definition is 'quantifiable'. Both the probabilities that a particular outcome occurs and its impact must be known. If the probabilities of different outcomes occurring are not known then we are working under conditions of **uncertainty**, not risk.

Note that the strict definition of risk allows for *good* outcomes as well as bad

For example, insurance companies mostly deal with risk. For example, they maintain detailed statistics of the following:

- The chance of a 20 year-old driver having an accident;
- The chance of a house burning down
- The chance of a burglary
- The chance that someone who is 70 dying within the next 10 years

Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (3.6.1.1) of occurrence.

If probabilities, or the chance of an event occurring are not known (uncertainty) then organisations and individuals are working much more in the dark.



## 2. Types of risk

Risk can be categorised using the following terms:

- **Pure risk:** this is where there is the chance of loss but no chance of a gain. It is also known as '**downside risk**'. Often when risk is mentioned, this is the type of risk meant, but remember that, strictly 'risk' is the spread of all results, good and bad. Examples of pure risk include: fire destroying a factory, an IT system being hacked, an employee being injured at work and fraudulent transactions by an employee.
- **Speculative risk:** this is where there can be both good and bad outcomes. It might occasionally be called '**two-way risk**'. Examples include developing a new product, entering a new market, buying a more advanced machine and developing a new web-site. Each of these good go well or badly.
- **Upside risk:** the possibility of making a gain.

## 3. Conformance and performance

Risks are an inevitable when running a business or other organisation. If a business were unable to take any risks it would not buy inventory (in case it wouldn't sell), it would not extend credit (in case of bad debts), and it would not employ anyone in case they were no good. The same applied in not-for-profit organisations such as a hospital (where surgeons would not operate in case the patient dies) or schools (where sports would be banned in case a pupil were injured).

Favourable outcomes for the organisation and its stakeholders are not available unless risks are undertaken. The key is the balance between the risk and the organisation's performance.



IFAC: seek to balance conformance and performance. Compliance is necessary to avoid failure, but it does not produce success.

Higher risks are needed if you are to produce higher returns. Compliance with rules, regulations and controls does not of itself make an organisation successful. However, poor conformance with controls and risk management strategies can certainly lead to organisational failure.

The aim of risk management is not to eliminate all risks: it is to understand and manage risks in line with shareholders' expectations about both risk and return.



A simple matrix can be used to illustrate the point:

		Risk	
		Low	High
Return/ Competitive advantage	Low	Routine	Avoid
	High	Identify and develop	Cautiously examine

Examples could be:

- Routine: extending moderate credit to a new customer. The maximum write-off of a debt would be small and the customer will provide some income.
- Avoid: entering a joint venture with a company that has a poor reputation. Returns might be small compared with the risk of the company's goodwill being tarnished.
- Identify and develop: support of a well-known charity or sporting event to improve the company's reputation. This could create a very large increase in competitive advantage and the risk would be low provided the third party were carefully chosen
- Examine cautiously: opening operations in a new country. There are considerable risks that the expansion might fail, but if it is successful the rewards could be huge.

## 4. Categorisation of risks

There are many ways in which risks can be categorised. In many ways this isn't important for its own sake but the categories can act as checklists when trying to identify and anticipate risks.

One categorisation is strategic, operational, reporting and compliance risks:

- **Strategic risks:** these arise from long term effects such as those relating to the nature and type of business, changes in competitive and legal environments, poor long-term decisions being made. For example, a supermarket which did not respond to the growing popularity of on-line shopping would have opened itself to a long-term decline in profits.
- **Operational risks:** short-term, day-to-day problems. For example, a machine breaking down, a key employee leaving, a fire breaking out in the warehouse or a fraud occurring.
- **Reporting risks:** risks arising because internal and external reporting are not reliable. For example, management accounts containing errors can lead to incorrect analysis and decisions.
- **Compliance risks:** the risks arising from not complying with rules and regulations. Penalties, loss or reputation and removal of operating licenses can all result.



Some major risks are set out below, just to give you an idea of the wide variety of risks that organisations might have to deal with. Each type of risk has one example given:

- Environmental: the release of dangerous chemicals into the local river.
- Economic: interest rates being increased so that consumer demand is suppressed.
- Competitor: a competitor launches a fantastic product.
- Product: you launch a poor product
- Commodity: the supply and price of raw materials change adversely.
- Political, cultural and legal: your product, for example cigarettes, becoming illegal or unpopular
- Financial (currency, interest rate, market risk, reporting): you are exporting and the buyer's currency weakens before you are paid.
- Investment: a subsidiary is bought but it turns out that it isn't as good as you thought it would be.
- IT: hacking and release of customer details
- Knowledge management: techniques and know-how aren't captured and recorded so that when employees move-on they leave little behind.
- Property: Fire, flood
- Health and safety risks: injury to employees and fines by regulators.
- Trading risks: irrecoverable debts.
- Resource risks: increasing difficulty recruiting the right people
- Organisational risks: the organisation is too moribund and too slow to respond to developments in the market.
- Inadequate system risks: management information inaccurate and out-of-date.
- Fraud risks: theft of cash or inventory.
- Probity risks (unethical behaviour): an employee acts unethically and the company's reputation is damaged.
- Reputational risks: products get a name for being unreliable so the company's reputation is damaged.



## 5. How much risk should an organisation take on?

'**Risk appetite**' is the term given to describe the amount of risk an organisation is willing to accept in pursuit of value.

Risk appetite is determined by two factors:

- Stakeholder's attitude to risk
- Risk capacity, which is the amount of risk that the organisation can bear.

Taking a personal example:

Some people are risk seekers and like to gamble; others are risk averse. So, if betting on a horse race, the risk seekers might be attracted to gamble on the high odds 100 to 1 horse. The risk averse person would tend not to consider that sort of gamble. They have different attitudes to risk.

However, let's say both people has \$100,000 in the bank and were being asked to bet \$100. Even the risk averse person might be tempted to go for 100 to 1 odds. In this situation they have high risk capacity because losing \$100 is of little consequence. But what if each person had only \$100 in the bank? There's a fair chance that neither would bet \$100 because the consequences of losing are so serious: they have very low risk capacity.

So, overall their appetite for risk (ie their appetite for the gamble) depends on their own attitudes plus the risk capacity.

## 6. Potential advantages of risk management

- More predictable cash flows
- Well-run systems (eg greater efficiency because routine maintenance is used to prevent the risk of machine breakdown).
- Limitation of the impact of disaster (eg, stand-by arrangements are in place to take over IT)
- Greater confidence amongst investors, employees, customers, suppliers and partners.
- Better matching to risk appetite of shareholders.

Remember organisations should obtain an acceptable balance between risk and return.

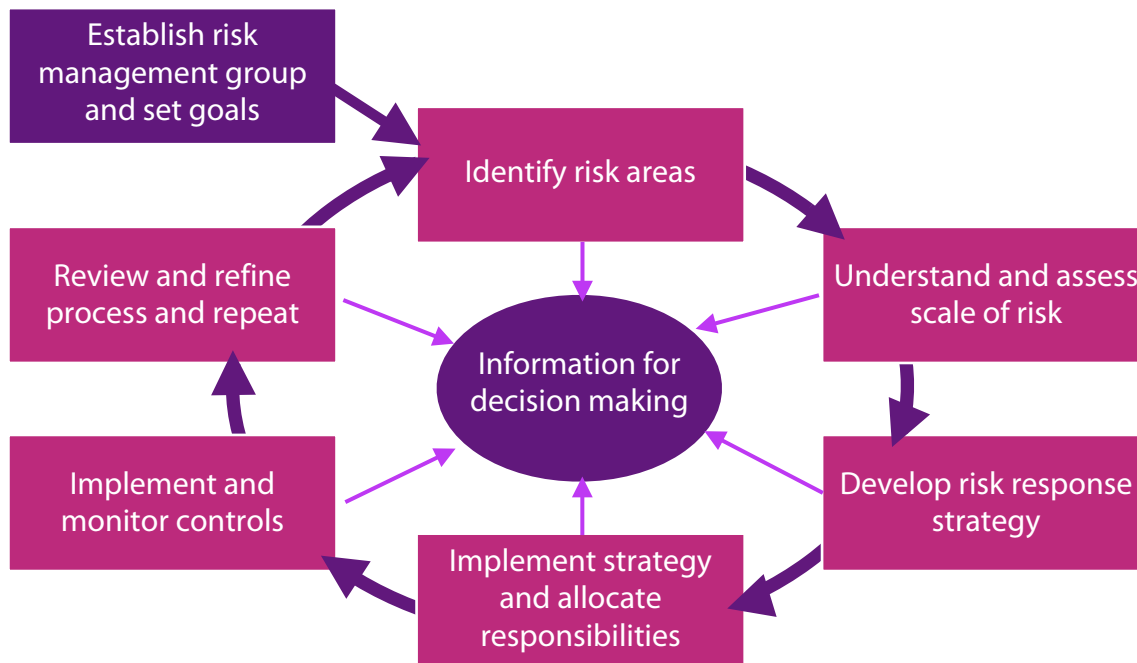




# Chapter 2

## RESPONSES TO RISK

### 1. A framework for risk management – the CIMA risk management cycle



The framework is logical and easy to understand.

- **Establish a risk management group and set goals**

Ultimately risk management is the responsibility of the board (or, more broadly, those charged with governance). However, like many functions in organisations the board is likely to delegate responsibility to a sub-group of suitable specialists. The board should set goals which reflect the risk appetite of the organisation. For example, if the organisation is an airline, the board would set goals of Zero accidents but it might be prepared to tolerate a degree of risk of bad publicity from over-booking flights.

- **Identify risk areas**

It is important not to be complacent about risks. Some will be obvious and well-known but others might be undiscovered until something goes wrong. We will see later in this Chapter methods that might help to discover potential risks.

- **Understand and assess the scale of the risk**

Not all risks are equal. Some risks that are discovered might be judged a being of little consequence; others could be of major significance. Techniques will be covered later.



- **Develop a risk response strategy**

Having identified and assessed the risks decisions have to be made about what to do about them. The TARA approach will be explained later.

- **Implement strategy and allocate responsibilities**

Simply identifying risks and working out suitable responses will not reduce risk: proper actions have to be specified must to be consistently carried out. For example, ensuring that the safety of machines is monitored or that customer credit limits are regularly reviewed. Individuals have to be put in charge of risk management strategies and procedures and must be held accountable for failures.

- **Implement and monitor controls**

Controls must then be implemented. For example, setting out dates by which risks have to be addressed, ensuring that inspections are done at regular intervals or by sending staff on training courses. It is very important to document risk reduction strategies and how those strategies are realised.

- **Review and refine the process and repeat**

Of course, the solutions implemented to deal with identified risks are unlikely to work perfectly the first time. They will often need to be improved. But it is also very important to realise that nothing stand still: risks will be evolving all the time and the organisation must keep them under constant review to ensure that all are properly addressed.



## 2. Identifying risk areas

The trick is to use every method at your disposal to identify risks. Throw the net as widely as you can at this stage. Later, risks might be dismissed as being of little importance, but it is important that as many as possible potential risks are initially considered.

### Methods include:

- Physical inspection and observation (for example, that safety equipment is still used on machinery).
- Inspect documents (for example, the accident log book).
- Internal audit. Internal auditors are employees of the company (usually) who examine and report on the organisation systems of internal control. Not only do they report on financial controls but they can also be required to examine systems such as quality control accident reporting and so on.
- Outside consultants brought in to audit procedures (for example, security consultants to advise on IT security).
- Observation of competitors' procedures (question why they carry out operations in a particular way).
- Enquiries (for example, ask employees, customers and suppliers about problems).
- Brainstorming (wide-ranging discussions to anticipate potential problems).
- Checklists (for example, use a checklist to evaluate how a job went and consider action where there had been problems).
- Benchmarking (falling short of targets can imply that things are going wrong).
- External events (for example, be alert for economic events that could affect the organisation).
- Internal events (for example, high staff turnover can indicate problems with employment conditions).
- Leading event indicators (for example, if a customer takes longer and longer to pay each month then there would appear to be a risk of non-payment).
- Escalation triggers (for example, if you are twice late filing a tax return, then the third default could be very serious).
- Event interdependencies (for example, a major customer going into liquidation could cause excess inventory problems).
- Scenario planning and stress testing (see below)



### 3. Scenario planning and stress testing

#### 3.1. Introduction

Scenario planning looks at all the things that could happen (and there can be many permutations of future events) and from those builds viable scenarios: a number of believable, internally consistent futures. This greatly reduces the number of 'universes' that need to be considered and allows the organisation to focus on the relatively few most likely scenarios.

It operates on the principle that, for some decisions, thinking in terms of multiple possible futures, or scenarios, is more effective than relying on single-point forecasts about the future.

For example, our political horizon might suggest that either Government 1 or Government 2 will be elected within the next year. Our economic predictions might suggest that interest rates will be either 3% or 5%. However, if Government 1 favours high public expenditure then this makes 5% interest rates much more likely as high interest rates are offered to allow government borrowing. If Government 2 favours austerity, then interest rates are likely to stay at 3%. Therefore, the only two viable scenarios are:

	Government 1	Government 2
Interest rates 3%	Not feasible	Yes
Interest rates 5%	Yes	Not feasible

- Government 1; 5%
- Government 2; 3%

Other permutations can be ignored because they are implausible.

#### 3.1. Steps in scenario planning

1. Define the scope, for example: What time horizon? Which part of the business? Which country (for multi-national organisations)?
2. Identify which factors will most affect the organisation.
3. What are the plausible outcomes for each factor?
4. What are the plausible, internally consistent combinations of factors?
5. What are the effects of these scenarios on the organisation's response?
6. How should the organisation respond? For example, it could decide to retreat to an Internet-only presence, it could move up-market/down-market, or it could withdraw from the market.
7. Go back and recheck assumptions and scenarios in the light of decisions made as some decisions might affect these.



### 3.2. Advantages and disadvantages of scenario planning

Scenario planning can have the following advantages:

- It challenges managers and other stakeholders to be more forward-looking when business planning.
- It challenges assumptions about the future, and about the drivers and forces that influence its industry sector.
- It forces managers to consider previously unimagined possibilities and tests the rational for current strategies.
- It does not attempt to forecast the future – almost certainly a lost cause. Instead it results in several outcomes, each of which can have a planned response.
- It encourages communication and planning within the company as scenario building requires inputs from many areas.
- It can encourage the identification and evaluation of 'weak signals'. Weak signals are small signs of changes that do not currently have much effect but which might be game-changing in the future. For example, early adopters of Facebook might have used it for purely personal use, but some might have foreseen the major effect it would have on marketing.

Scenario planning can have the following disadvantages:

- It can be very time-consuming: identification of all the relevant variables, collection of data and the distillation to a few plausible, internally consistent scenarios.
- It is important to use experts who can assess possible outcomes – and the cost of experts' time can be considerable.
- It is important not to eliminate all scenarios except the most likely one or the most attractive one. The point of scenario planning is to obtain a range of possibilities – both favourable and unfavourable - and to plan for those.



## 4. Stress testing strategy

If there is one certainty in business it is that strategic plans rarely produce outcomes that are precise matches for the original plan. A strategic plan has a time horizon of around five years and an awful lot can happen in that time. So, what happens if unfavourable events occur? Will the company survive? Does the strategic plan have enough flexibility build into it so that it can be adapted part way through? Are there enough resources (such as cash) to see the company safely through bad times? Stress-testing attempts to identify risks and scenarios that might occur to help organisations understand where vulnerabilities exist and to build in risk resilience.

A stress test is, therefore, an assessment of how a system or strategy is likely to function if severe adverse events occur. For example, would your company survive if your major customer went into liquidation? What would happen if a major product had to be withdrawn (at the time of writing Boeing has had to ground all its 737 Max 8 jets after two similar accidents involving nearly new planes and, no doubt, airlines using those planes will ask for compensation). What would happen if a monopoly supplier of a vital component were taken over by one of your rivals?

Stress tests should be carried out on all strategies, whether an existing strategy is being followed (perhaps it has become high risk) or a new strategy is planned.

Of course, there will always be a problem envisioning all the things that can go wrong and deciding if their probabilities are significant and many organisations can disapprove of the Jeremiahs in their midst who think about calamity when the rest of the organisation is expected to embrace enthusiastically and, perhaps sycophantically, the board's new strategy.

It is therefore important that in the rules and culture of the organisation stress-testing becomes a mandatory and valued.

There are many potential approaches to stress testing, but the following list is as helpful as any:

- Look to the future. What consumer trends, technical developments and political changes might occur and which will affect the business. Going through the PESTEL headings and projecting these into their possible future effects on the business can be a good start. Don't flinch from unpleasant possibilities or engage in wishful thinking: evaluate events' likelihood and their effects.
- Understand what makes your business currently successful. Understand your value chain and what you are good at. What would happen if your unique capability in an important area were to disappear? For example, if you were a pharmaceutical firm, what will happen when your patent on a block-buster drug runs out? If you are a car manufacturer, what would happen if a competitor discovers a battery technology that increases range by a factor of 10? What happens if you a firm of lawyers and artificial intelligence develops to such a degree that reliable advice can be offered on line and perhaps even disputes can be judged on-line?
- Does the strategy embody objectives? If there are no objectives (eg following the SMART pattern of specific, measurable, achievable, relevant and time-limited) then the strategy is useless as it will not be achieved.
- Is the strategy an incremental change to the current strategy (relatively safe) or a radical departure (relatively dangerous)? Sometimes a radical approach is needed to save businesses but be aware that the company is then venturing into areas where it will have little expertise or market knowledge. Assumptions and feasibility have to be examined much more critically.
- Have stakeholders bought into the strategy? If there are powerful dissenters then the strategy will probably not work.
- Does the new strategy offer the hope of adding value for customers?



- Set up a financial model and change the parameters and assumptions used to examine how sensitive success or survival is to each. We can all produce cash flow forecasts on a spreadsheet which allows our company to live within its overdraft limit. Simply change assumptions about sales, costs etc until you get the required answer. But that is no way to stress test? Be at least realistic, then be pessimistic. No reward will come without risk, but at least understand the risks arising from the strategy.

So, questions that could be asked and scenarios that could be played out could include:

- What happens if interest rates double?
- What happens if there is a serious recession?
- What would happen if our major customer failed?
- What would happen if a major product was discovered to have a serious flaw?
- What happens if a competitor makes an important technical breakthrough?

These can be built into sets of viable, if unpleasant, scenarios and the company can then respond however it sees fit.



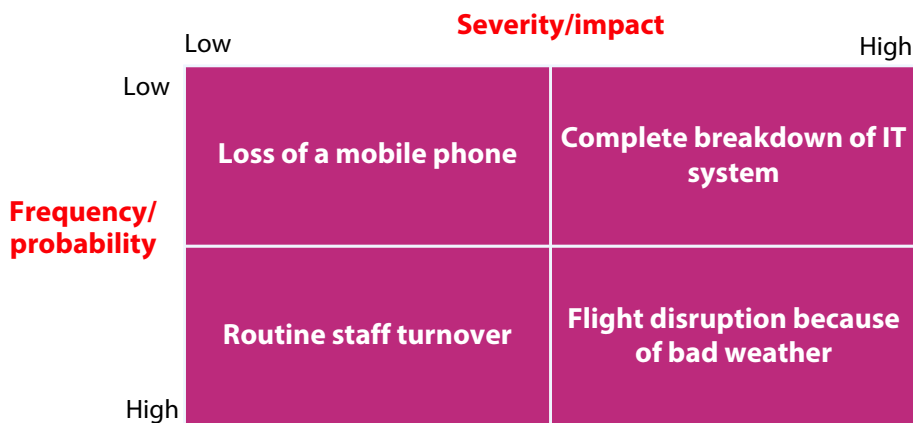
## 5. Understand and assess the scale of the risk

The scale of the risk depends on:

- (1) The likelihood that the event will occur; and
- (2) The impact of the event.

Of course, these will be estimates, particularly the probability of an event occurring. However, precise figures are not needed, just an idea of whether they are 'high' or 'low'. Nevertheless you will see some mathematical techniques that can be used to quantify events.

A very standard tool to assess the scale of the risk is a **risk map** (or assurance map):



Note that there is nothing absolute about the categorisation of these risks. For example, the chance of flight disruption has been assessed as high, but that depends on the airports used. Similarly, the loss of a mobile has been categorised as being of low impact – but this wouldn't be correct if that mobile was the only place where important contact data is held.

The severity of the risk can be estimated by methods such as:

- **Calculation of average/expected loss, largest predictable loss**
- **Exposure of physical assets: total loss, repair, decrease in value**
- **Exposure of financial assets**
- **Exposure of human assets (injury, death, staff leaving)**

Obviously, great attention should be given to risks in the bottom right hand quadrant (high/high) whereas those risks in the top left quadrant are less important.



## 6. Risk response

The risk responses can be remembered by the TARA approach:

<b>Transfer</b>	Methods of transferring risk include insurance, sub-contracting operations or joint ventures (partial transferring). Insurance is, for example, used to protect against risk in motoring accidents. Individuals do not have bad accidents often, but if they do the consequences can be very severe.
<b>Avoid</b>	The risk has been assessed as being so serious that all possibility of the event occurring should be avoided.
<b>Reduce</b>	Take steps to mitigate the risk. For example, instead of installing a new computer system in every branch over one weekend, run a pilot operation then gradually extend.
<b>Accept</b>	Don't do anything about the risk. It's just part of everyday business

(You might occasionally see these approaches referred to as the 4Ts: Transfer, terminate, treat, tolerate.)

The four responses can be mapped onto the risk map diagram as follows:

		Severity/impact	
		Low	High
Frequency/probability	Low	Loss of a mobile phone <b>ACCEPT</b>	Complete breakdown of IT system <b>TRANSFER</b>
	High	Routine staff turnover <b>REDUCE</b>	Flight disruption because of bad weather <b>ABANDON</b>

So, phones are lost (or stolen) from time to time and most people live with that risk (though insurance is always a possibility and might be taken out for very expensive phones).

The complete breakdown of an IT system could be dealt with by outsourcing the system so the supplier shoulders the risk.

Routine staff turnover has costs associated with it (recruitment and training) so better employment policies might be worthwhile to reduce the cost and disruption.

Flights to an airport with very bad weather or safety records might simply be abandoned because they cause more trouble than they are worth.

## 7. Gross and net risks

It is important to know these terms:

**Gross risk** = the risk before any mitigation (reduction) procedures. Gross risk is sometimes referred to as **inherent risk**.

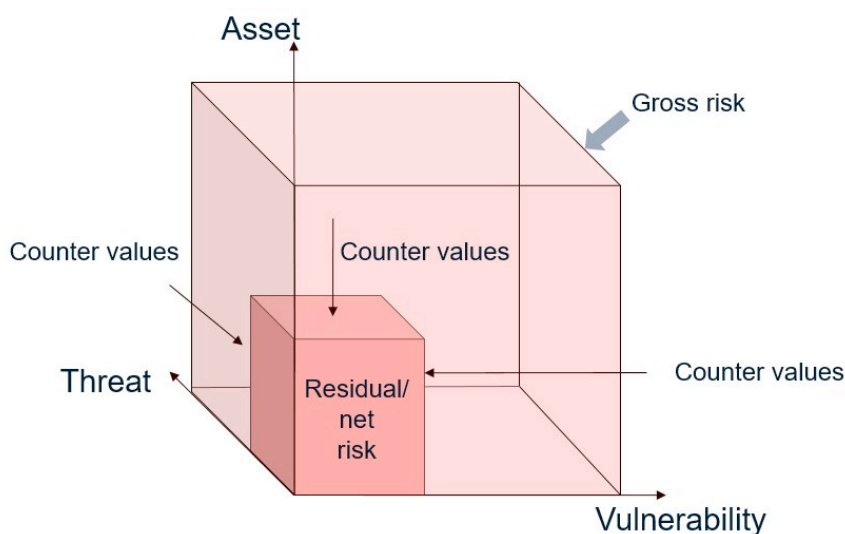
**Net risk** = the residual risk after reduction and mitigation.

The gross risk is initially dependent on:

- **The asset:** what you are trying to protect. For example, property, cash, people, reputation and so on.
- **The threat:** what you are trying to protect against. For example, destruction of property, theft of cash, injury to people, damage to reputation.
- **The vulnerability:** weaknesses or gaps that can be exploited. For example, no fire alarms, cash not banked, no hand rails on stairs, poor PR.

The gross risk can be reduced to a lower net risk, or residual risk by reducing any of these variables through the application of counter-values or counter-measures.

**Management must then decide whether the residual risk is within the organisation's risk appetite.**



Examples:

**Asset:** the inventory in warehouse; **threat:** fire; **vulnerability:** full of inflammable material

Counter values could be:

**Asset:** reduce the amount of inventory

**Threat:** impose no-smoking rules (if not already present),

**Vulnerability:** install smoke detectors and a fire suppression system that is suitable for the type of inventory stored.



**Asset:** valuable sales manager; threat: moves to a competitor; vulnerability: enticing offers from competitors.

Counter values could be:

**Asset:** divide sales over two managers (each person is half as valuable).

**Threat:** impose contracts that require 3 – 6 months' notice to make moving more difficult

**Vulnerability:** offer good pay, conditions and prospects.

## 8. The risk register

Identified risks, their probability of occurrence, impact and responses to them should be entered into a **risk register**. Typical contents of a risk register are:

- Description of the risk
- Date identified
- Its estimated likelihood of occurrence before mitigation
- Its likely impact before mitigation
- Pre-mitigation rating
- The risk owner (who is responsible for dealing with the risk)
- Detailed response strategy to the risk (TARA)
- Its estimated likelihood of occurrence after mitigation
- Its likely impact before mitigation after mitigation
- Post mitigation rating
- Date by when response should be implemented
- Date response implemented
- Signed off by risk owner

The board and risk management committee should take an active interest in the risk register to ensure that identified risks have been satisfactorily dealt with.

## 9. Assurance mapping

Risk identification and risk mapping identify the problems and their severity, but those processes are a waste of time if suitable responses are not made. The risk register is one way to record risks and to assign responsibilities for mitigating the risks where necessary. Another approach to ensure that risks are properly dealt with is to construct an assurance map. The aim of an assurance map is to identify where the safeguards against risks are to be found.

Assurance maps identify that an organisation has various lines of defences against risk. Typically these are:



Line of defence	Source
1st line of defence	Management-based assurance. For example, board policies and management review.
2nd line of defence	Internal procedures and legal-based assurance. For example, health and safety legislation, risk registers, compliance with reporting requirements, procedures and quality control tests.
3rd line of defence	Independent assurance. For example, internal audit, external audit, actuaries, consulting engineers, legal opinions.

Note that some organisations might identify slightly different lines of defence.

A table is then drawn up listing the risks, their importance and how the lines of defence deal with those risks. For example

Type of risk	First line of defence	Second line of defence	Third line of defence
Finance: sufficiency and gearing			
IT			
Human resources			
etc			

Here, black depicts strong assurance, grey depicts middle assurance and white depicts no assurance.

Sometime an additional column is added to show the desired amount of defence against risks.

Each row is then scrutinised to ensure that the appropriate defences are in place somewhere in the lines of defences to provide sufficient overall assurance that each risk has been sufficiently countered.



# Chapter 3

## ENTERPRISE RISK MANAGEMENT

### 1. Introduction

**Enterprise Risk Management (ERM) can be defined as the:**

'... process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.'

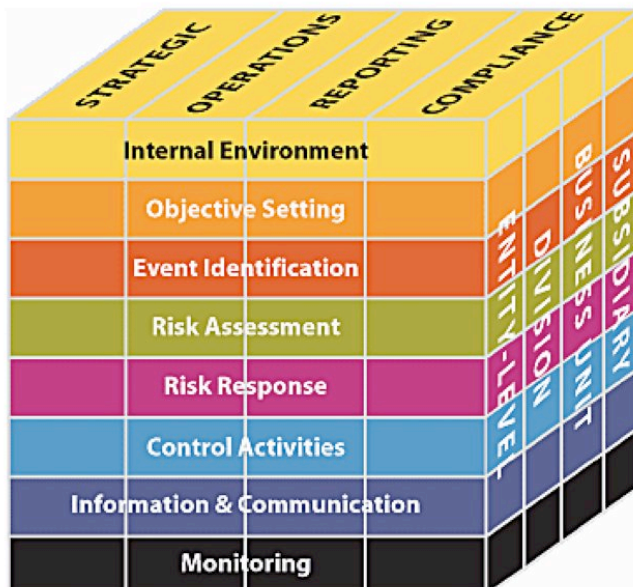
Enterprise Risk Management – Integrated Framework,  
the Committee of Sponsoring Organisations, COSO, 2004

The CIMA Official Terminology uses the COSO (Committee of Sponsoring Organisations) definition.

Think of ERM as a development and formalisation of the approaches already described.

### 2. The COSO framework for ERM

The following diagram sets out the COSO framework for ERM:



Across the top of the cube are all the categories of risk that an enterprise can suffer from: strategic, operations, reporting and compliance. These have already been discussed.

Down the side, going "into" the paper the enterprise is considered at various levels of operation: the whole entity (think of group level); divisional level (Eg European, USA and Asian divisions); then

business units (such as cars and commercial vehicles); finally subsidiaries (for example, different marques of car).

Some risks will be felt at entity level – for example, the Volkswagen exhaust emission scandal. Other risks will be more limited - for example, one make and model of vehicle that has to be recalled for repair, or a subsidiary dealing with consumer finance for new vehicles not complying with lending regulations.

**Risk consolidation** is the process of aggregating divisional/subsidiary risks at the corporate level. Some risks can be handled together and be subject to a common approach, or they might even substantially cancel.

For example, many organisations will organise insurance at the group level to cover injury to employees anywhere in the group. This approach will usually be cheaper than insuring small groups of employees separately.

Similarly, if one subsidiary is exporting and receiving US\$, whilst another is importing and spends US\$, the net exposure to US\$ currency movement might be very low and can be ignored at the group level.

**Down the front of the cube are the elements of a risk management approach:**

#### ● **Internal environment**

This can be regarded as the outlook and culture of the organisation, including its enthusiasm for risk management and its risk appetite.

For example, some organisations are a bit happy-go-lucky when it comes to risk management whereas others are extremely strict and want things to be done by the book.

#### ● **Objective setting**

Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

For example, the objectives of a military operation might be to capture a town and to do that, certain risks will be experienced and have to be assessed and evaluated.

The objectives of a research and development department in a business will establish the risks that it suffers (such as a development failing to work).

The objectives of a marketing department will, again be quite different, and will be judged against their risks such as the failure of a marketing campaign (or too much uptake on special offers!)

#### ● **Event identification**

As discussed earlier, there are internal and external events (both positive and negative) which affect the achievement of an entity's objectives and must be identified.



### ● Risk assessment

As already discussed, risks are analysed to consider their likelihood and impact as a basis for determining how they should be managed.

### ● Risk response

Management selects risk response(s) to transfer, avoid, reduce or accept risk (TARA).

The aim is to align risks with the entity's **risk tolerance** and risk appetite. Risk tolerance is the acceptable variation in outcome compared to an original objective. In setting risk tolerance, management considers the relative importance of the related objective. So, if an objective is particularly important, risk tolerances might be higher to recognise that achieving something really worthwhile is worth accepting more risk.

### ● Control activities

Policies, procedures and control methods help to ensure risk responses are properly carried out. Examples of control activities include authorisation of transactions, reconciliations, segregation of duties (splitting a transaction so that several people are involved), physical controls (such as locking away valuable inventory), the comparison of actual results to budgets. IT controls can also be very important.

### ● Information and communication

Information that monitors or identifies risks must be identified, recorded and communicated quickly enough and in a way that lets people carry out their responsibilities by making decisions. For example, if a product's sales are lower than expected, this information must be available quickly enough to change prices, alter the advertising campaign – or to withdraw the product.

### ● Monitoring

The entire ERM process must be monitored and modifications made as necessary, to improve current methodologies and to adapt to emerging risks, so that the system stays relevant.

## 3. Risk reports

UK quoted companies are now required to include risk reports as part of their annual reports. This informs shareholders and others about the organisations' main risks and what the company is doing about them.

Here is an *extract* from Unilever's 2015 report and financial statements:

[https://www.unilever.com/Images/governance\\_and\\_financial\\_report\\_ar15\\_tcm244-477381\\_en.pdf](https://www.unilever.com/Images/governance_and_financial_report_ar15_tcm244-477381_en.pdf)



## 4. Principal Risk Factors

Our business is subject to risks and uncertainties. On the following pages we have identified the risks that we regard as the most relevant to our business. These are the risks that we see as most material to Unilever's business and performance at this time.

There may be other risks that could emerge in the future. We have also commented below on certain mitigating actions that we believe help us to manage these risks. However, we may not be successful in deploying some or all of these mitigating actions.

If the circumstances in these risks occur or are not successfully mitigated, our cash flow, operating results, financial position, business and reputation could be materially adversely affected. In addition, risks and uncertainties could cause actual results to vary from those described, which may include forward-looking statements, or could affect our ability to meet our targets or be detrimental to our profitability or reputation.

DESCRIPTION OF THE RISK	WHAT WE ARE DOING TO MANAGE THE RISK
<b>BRAND PREFERENCE</b>  <b>As a branded goods business, Unilever's success depends on the value and relevance of our brands and products to consumers around the world and on our ability to innovate and remain competitive.</b>  Consumer tastes, preferences and behaviours are constantly changing and Unilever's ability to anticipate and respond to these changes and to continue to differentiate our brands and products is vital to our business.  We are dependent on creating innovative products that continue to meet the needs of our consumers. If we are unable to innovate effectively, Unilever's sales or margins could be materially adversely affected.	We continuously monitor external market trends and collate consumer, customer and shopper insight in order to develop category and brand strategies.  Our strategy focuses on investing in markets and segments which we identify as attractive because we have already built, or are confident that we can build, competitive advantage.  Our Research and Development function actively searches for ways in which to translate the trends in consumer preference and taste into new technologies for incorporation into future products.  Our innovation management process deploys tools, technologies and resources to convert category strategies into projects and category plans, develop products and relevant brand communication and successfully roll out new products to our consumers.



## SUPPLY CHAIN

**Our business depends on purchasing materials, efficient manufacturing and the timely distribution of products to our customers.**

Our supply chain network is exposed to potentially adverse events such as physical disruptions, environmental and industrial accidents or bankruptcy of a key supplier which could impact our ability to deliver orders to our customers.

The cost of our products can be significantly affected by the cost of the underlying commodities and materials from which they are made. Fluctuations in these costs cannot always be passed on to the consumer through pricing.

We have contingency plans designed to enable us to secure alternative key material supplies at short notice, to transfer or share production between manufacturing sites and to use substitute materials in our product formulations and recipes.

These contingency plans also extend to an ability to intervene directly to support a key supplier should it for any reason find itself in difficulty or be at risk of negatively affecting a Unilever product.

We have policies and procedures designed to ensure the health and safety of our employees and the products in our facilities, and to deal with major incidents including business continuity and disaster recovery.

Commodity price risk is actively managed through forward buying of traded commodities and other hedging mechanisms. Trends are monitored and modelled regularly and integrated into our forecasting process.

## SAFE AND HIGH QUALITY PRODUCTS

**The quality and safety of our products are of paramount importance for our brands and our reputation.**

The risk that raw materials are accidentally or maliciously contaminated throughout the supply chain or that other product defects occur due to human error, equipment failure or other factors cannot be excluded.

Our product quality processes and controls are comprehensive, from product design to customer shelf. They are verified annually, and regularly monitored through performance indicators that drive continuous improvement activities. Our key suppliers are externally certified and the quality of material received is regularly monitored to ensure that it meets the rigorous quality standards that our products require.

In the event of an incident relating to the safety of our consumers or the quality of our products, incident management teams are activated in the affected markets under the direction of our product quality, science, and communication experts, to ensure timely and effective market place action.



## 5. Environmental, social, and ethical issues of risk management

Organisations affect their environment and the human stakeholders with whom they interact. These effects can often produce ethical dilemmas that organisations have to deal with.

### Examples of environmental issues

- BP and the Deepwater Horizon oil spill in the Gulf of Mexico
- VW and car emission misreporting
- Release of dangerous chemicals into water supplies

Everyone is wise with hindsight and no-one in the organisations concerned would have wanted these events to happen (though someone in VW was responsible for incorrect reporting).

However, as always, there is a balance to be struck between risk and performance. Quite obviously there would be no oil spills if no company drilled for oil. BP had safety procedures in place but either they were inadequate or BP suffered exceptional bad luck. Not only did the company have to pay huge fines and compensation (about \$60Bn) but it suffered severe reputational damage.

Unilever's risk report also contains a section on sustainability:

### SUSTAINABILITY

**The success of our business depends on finding sustainable solutions to support long-term growth.**

Unilever's vision to accelerate growth in the business while reducing our environmental footprint and increasing our positive social impact will require more sustainable ways of doing business. This means reducing our environmental footprint while increasing the positive social benefits of Unilever's activities. We are dependent on the efforts of partners and various certification bodies to achieve our sustainability goals. There can be no assurance that sustainable business solutions will be developed and failure to do so could limit Unilever's growth and profit potential and damage our corporate reputation

The Unilever Sustainable Living Plan sets clear long-term commitments to improve health and well-being, reduce environmental impact and enhance livelihoods. Underpinning these are targets in areas such as hygiene, nutrition, sustainable sourcing, fairness in the workplace, opportunities for women and inclusive business as well as greenhouse gas emissions, water and waste. These targets and more sustainable ways of operating are being integrated into Unilever's day-to-day business.

Progress towards the Unilever Sustainable Living Plan is monitored by the Unilever Leadership Executive and the Boards. The Unilever Sustainable Living Plan Council, comprising six external specialists in sustainability, guides and critiques the development of our strategy.



## Examples of social issues

- Use of Facebook, Twitter to 'troll' and bully.
- Capture of 'big data' to analyse consumer habits
- Discrimination or lack of diversity in the workplace

Companies suffer reputation risk if their products or information gathering cause damage. The unauthorised release of data can cause financial damage to customers.

Poor recruitment policies leave companies open to accusations of discrimination and this can cause both reputational damage and can lead to legal claims.

Poor diversity policies can cause poor business results as products, services and employees no longer match up to what customers expect.

## Ethical issues

For example, a pharmaceutical company is developing a new drug. Some of the ethical issues arising from this are:

Safeguarding the volunteers on whom the drug is tested

How much testing should be done before the drug is marketed? The more testing the greater the delay in releasing a drug very effective in treating a disease but, balancing that, more testing means less chance of undiscovered side effects.

What price should the drug be sold at? A high price might please shareholders and could enable more money to be spent on research and development of more drugs. However, a high price would mean that some patients and health services could not afford the drug. Should different prices be charged for the same drug in different countries depending on the country's wealth? Poor ethical choices present risks, particularly reputational and compliance.





# Chapter 4

## SOME QUANTITATIVE TECHNIQUES

### 1. Introduction

This chapter looks at some techniques which can be used to assess the probability or effect of a risk event.

Methods covered are:

- Expected values
- Value at risk
- Sensitivity analysis
- Risk adjusted discount rates
- Certainty equivalents
- Linear regression
- Simulation modelling

### 2. Expected values

Here is a simple expected values example. The expected value outcome is the sum of individual outcome weighted by the probability of each occurring. So here there are two states of the world (such as the economy doing well or poorly) and two once-off projects the company could invest in.

<i>State of the world</i>	<i>P</i>	<i>Project A income (\$)</i>	<i>Project B income (\$)</i>	<i>P x income of Project A</i>	<i>P x income of Project B</i>
I	0.6	2,000	4,000	1,200	2,400
II	0.4	10,000	6,500	4,000	2,600
			Expected values	5,200	5,000



The conventional advice as to which project to invest in would be to invest in Project A as it has the higher expected value. However, you need to be careful about a number of factors:

- (1) How have the probabilities been assessed? This must be very difficult in practice. Think about how inaccurate opinion polls are at predicting election results.
- (2) For a once-off projected the expected value is often (as here) not expected. The expected incomes are \$2,000 or \$10,000 for Project A and \$4,000 or \$6,500 for Project B
- (3) Expected values conceal risk. Say that each project cost \$3,800. There is no prospect (as far as is estimated) of Project B making a loss whereas Project A has a better than evens chance of earning only \$2,000 so that it would then make a loss of \$1,800 – which could be fatal for the company.

Because risk is concealed in expected values it is perhaps not the best tool to use for project appraisal

### 3. Sensitivity to probability assumptions

Just consider Project A above. Although the expected value is positive, it could result in the project making a loss if the probabilities had been incorrectly calculated. We can work out how the probabilities would need to change for the project to break even.

Instead of using the probability estimates of 0.6 and 0.4, let them be  $p$  and  $1 - p$  (note that they must add back to 1 to ensure all outcomes have been included). Project A can now be represented as:

State of the world	P	Project A income (\$)	P x income of Project A
I	$p$	2,000	$2,000p$
II	$1-p$	10,000	$10,000 - 10,000p$
		Expected value	$10,000 - 8,000p$

If the project is to break-even, the expected value of the outcome will equal to its cost of \$3,800.

$$\text{So, } 3,800 = 10,000 - 8,000p$$

$$8,000p = 10,000 - 3,800 = 6,200$$

$$P = 0.775$$

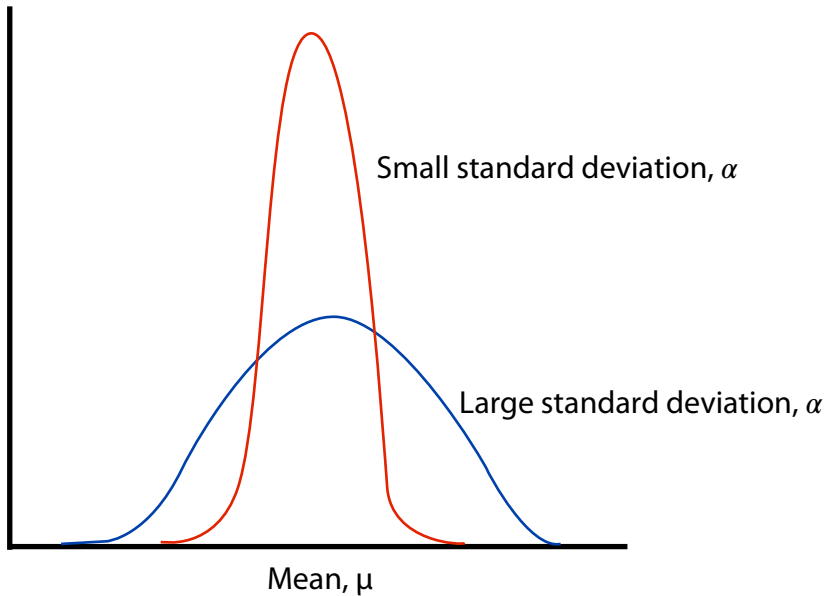
So if the probability of state of the world I occurring rose from 0.6 to 0.775, Project A would break even in present value terms. If the probability rose further, Project A's expected value would be less than the cost of the project.



## 4. Value at risk – introduction

In your exam it is assumed that results from an investment or the value of a share portfolio has a mean (average) value but that results vary around that mean following a normal distribution curve. This will allow estimates to be made of the likelihood of possible outcomes.

Normal curves have the following general shape:



If the possible results are closely clustered around the mean the standard deviation of the distribution is small; if the results are very spread out, the standard deviation of the distribution is large.

So if the mean daily value of a share is \$30 and the standard deviation of its value is \$1 the share is rarely valued very far from \$30. If, however, the standard deviation were \$10, then the share's value would be very volatile, often worth more than, say, \$40 and less than say \$20.

Because all normal curves are of the same basic shape, they can be described using a set of tables, as set out below.

The area under the curve holds all possible results and the table gives the proportion of those results between the mean and Z standard deviations above (or below) the mean

Note, Z is the distance above or below the mean expressed as a number of standard deviations, so for a value x, Z is:

$$Z = \frac{x - \mu}{\sigma}$$

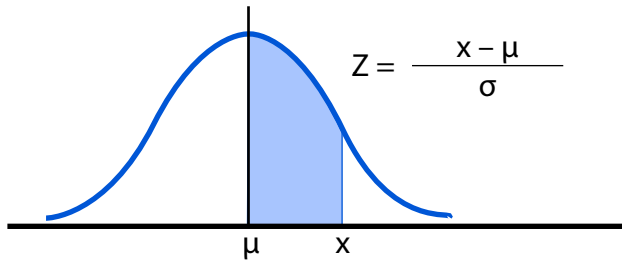
So, if the mean height of a population was 178 cm with a standard deviation of 4cm, we can work out what proportion of the population is 178 – 181 cm tall.

$$Z = \frac{181 - 178}{4} = 0.75$$

Look up the table value for Z = 0.75 by going down the left hand column until you get to 0.7, then across until you get to 0.05 and the table figure is 0.2734. That means 27.34% of the population is in



the height range 178 – 181 cm tall. Because the curve is symmetrical, the same proportion of people would be 175 – 178 cm tall.



Z	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.0000	0.0040	0.0080	0.0120	0.0160	0.0199	0.0239	0.0279	0.0319	0.0359
0.1	0.0398	0.0438	0.0478	0.0517	0.0557	0.0596	0.0636	0.0675	0.0714	0.0753
0.2	0.0793	0.0832	0.0871	0.0910	0.0948	0.0987	0.1026	0.1064	0.1103	0.1141
0.3	0.1179	0.1217	0.1255	0.1293	0.1331	0.1368	0.1406	0.1443	0.1480	0.1517
0.4	0.1554	0.1591	0.1628	0.1664	0.1700	0.1736	0.1772	0.1808	0.1844	0.1879
0.5	0.1915	0.1950	0.1985	0.2019	0.2054	0.2088	0.2123	0.2157	0.2190	0.2224
0.6	0.2257	0.2291	0.2324	0.2357	0.2389	0.2422	0.2454	0.2486	0.2517	0.2549
0.7	0.2580	0.2611	0.2642	0.2673	0.2704	0.2734	0.2764	0.2794	0.2823	0.2852
0.8	0.2881	0.2910	0.2939	0.2967	0.2995	0.3023	0.3051	0.3078	0.3106	0.3133
0.9	0.3159	0.3186	0.3212	0.3238	0.3264	0.3289	0.3315	0.3340	0.3365	0.3389
1.0	0.3413	0.3438	0.3461	0.3485	0.3508	0.3531	0.3554	0.3577	0.3599	0.3621
1.1	0.3643	0.3665	0.3686	0.3708	0.3729	0.3749	0.3770	0.3790	0.3810	0.3830
1.2	0.3849	0.3869	0.3888	0.3907	0.3925	0.3944	0.3962	0.3980	0.3997	0.4015
1.3	0.4032	0.4049	0.4066	0.4082	0.4099	0.4115	0.4131	0.4147	0.4162	0.4177
1.4	0.4192	0.4207	0.4222	0.4236	0.4251	0.4265	0.4279	0.4292	0.4306	0.4319
1.5	0.4332	0.4345	0.4357	0.4370	0.4382	0.4394	0.4406	0.4418	0.4429	0.4441
1.6	0.4452	0.4463	0.4474	0.4484	0.4495	0.4505	0.4515	0.4525	0.4535	0.4545
1.7	0.4554	0.4564	0.4573	0.4582	0.4591	0.4599	0.4608	0.4616	0.4625	0.4633
1.8	0.4641	0.4649	0.4656	0.4664	0.4671	0.4678	0.4686	0.4693	0.4699	0.4706
1.9	0.4713	0.4719	0.4726	0.4732	0.4738	0.4744	0.4750	0.4756	0.4761	0.4767
2.0	0.4772	0.4778	0.4783	0.4788	0.4793	0.4798	0.4803	0.4808	0.4812	0.4817
2.1	0.4821	0.4826	0.4830	0.4834	0.4838	0.4842	0.4846	0.4850	0.4854	0.4857
2.2	0.4861	0.4864	0.4868	0.4871	0.4875	0.4878	0.4881	0.4884	0.4887	0.4890
2.3	0.4893	0.4896	0.4898	0.4901	0.4904	0.4906	0.4909	0.4911	0.4913	0.4916
2.4	0.4918	0.4920	0.4922	0.4925	0.4927	0.4929	0.4931	0.4932	0.4934	0.4936
2.5	0.4938	0.4940	0.4941	0.4943	0.4945	0.4946	0.4948	0.4949	0.4951	0.4952
2.6	0.4953	0.4955	0.4956	0.4957	0.4959	0.4960	0.4961	0.4962	0.4963	0.4964
2.7	0.4965	0.4966	0.4967	0.4968	0.4969	0.4970	0.4971	0.4972	0.4973	0.4974
2.8	0.4974	0.4975	0.4976	0.4977	0.4977	0.4978	0.4979	0.4979	0.4980	0.4981
2.9	0.4981	0.4982	0.4982	0.4983	0.4984	0.4984	0.4985	0.4985	0.4986	0.4986
3.0	0.4987	0.4987	0.4987	0.4988	0.4988	0.4989	0.4989	0.4989	0.4990	0.4990

The use of the tables can be turned round to answer a question such as in what height range are the 20% of who are people just taller than the mean. This means that the shaded area in the diagram shown as part of the table has to be 0.2 as that represents the 20% of people just taller than the mean.



To solve this go to the 'body' of the table and look for 0.2. You will see that this is somewhere between  $Z = 0.52$  and  $0.53$  (areas = 0.1985 and 0.2019). In fact, 20% seems almost mid-way, so  $Z$  would be estimated at 0.525.

Using the formula at the top of the table:

$$Z = 0.525 = \frac{x - 178}{4} = 0.75$$

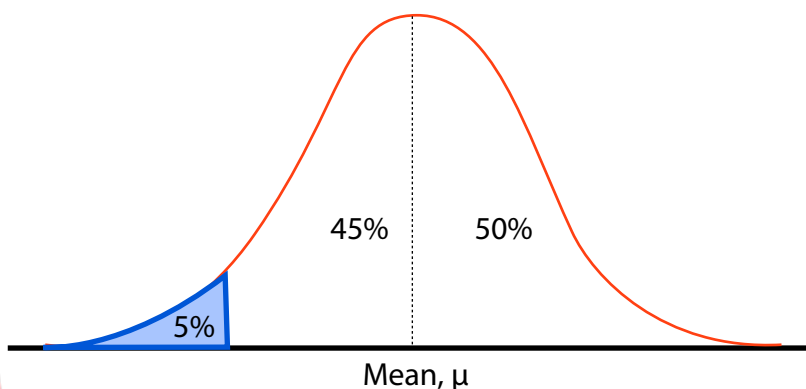
So,

$$x - 178 = 4 \times 0.525 = 2.1.$$

Therefore the 20% of people just taller than the mean of 178 cm will be in the height range 178 – 180.1 cm.

## 5. Value at risk – share values

What talking about value at risk, the commonest criterion is to work out the amount you could lose over a period so that there is only a 5% chance of losing more. This can be represented as follows on the curve:



We are looking for where the cut-off is to leave only the 5% lowest values.

Let's say that a shareholding has a mean value of \$80,000 and the daily has a standard deviation of \$5,000. The shareholding could easily have a value of \$81,000, \$78,000 and so on but you would have had some bad luck if tomorrow's value were only \$60,000. However, that low value would be possible.

So, below what value would only 5% of results lie?

5% splits the left hand side of the curve into 5%/45%, or 0.05/0.45. The normal curve tables give the area under the curve from the mean down or the mean up so would indicate the  $Z$  value for an area of 0.45.

Looking at the body of the tables for an area of 0.45, you will see that  $Z = 1.645$  (mid-way between 1.64 and 1.65).

$$Z = 1.645 = \frac{80,000 - x}{5,000} \quad (Z \text{ is the distance below the mean as a number of standard deviations})$$

$$5,000 \times 1.645 = 80,000 - x$$

$$x = 80,000 - 5,000 \times 1.645 = \$71,775.$$

So, there is only a 5% chance that after one day the shares will be worth less than \$71,775. There is a 95% chance that the shares will be worth more than that.

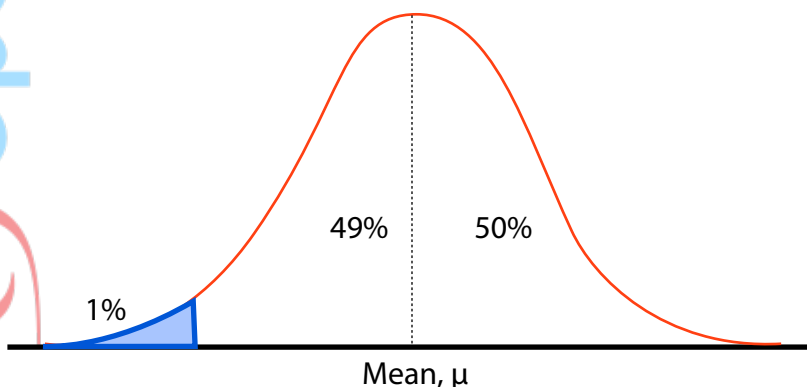
Another way of expressing that is to say that we are 95% confident that the shares will not be worth less than \$71,775.

The **value at risk** (VAR) at the 95% confidence level is the maximum you stand to lose with a 95% confidence, so that figure is:

$$80,000 - 71,775 = \$8,225$$

$$\text{Alternatively, the value at risk is simply } 1.645 \times \$5,000 = \$8,225$$

If you were asked to calculate the VAR to the 99% confidence level, then you are splitting the curve into 0.01, 0.49, 0.50 areas



The 49% (or 0.49) area needs to be found in the body of the tables (remember tables only give the area from the mean up or down) and the  $Z$  value for 0.49 is about 2.33.

$$Z = 2.33 = \frac{80,000 - x}{5,000} \quad (Z \text{ is the distance below the mean as a number of standard deviations})$$

$$5,000 \times 2.33 = 80,000 - x$$

$$x = 80,000 - 5,000 \times 2.33 = 68,350$$

So, there is only a 1% chance of the shares being worth less than \$68,350.

The value at risk to the 99% confidence level is  $80,000 - 68,350 = \$11,650$

This means that there is only a 1% chance of the shares losing more than \$11,650 in the course of a day.



## 6. Value at risk for several periods

The example above dealt with variations in share value over the course of a day and the standard deviation of \$5,000 was for one day. But what if we wanted to work out similar statistics for, say, a period of 10 consecutive days?

What we need now is a standard deviation for share value for 10 days.

The rule is (really you just have to learn this) is:

$$\sigma_{\text{period}} = \sigma_{\text{day}} \sqrt{n}$$

where n is the number of days in the period.

So, is the standard deviation of share value for 1 day is \$5,000, for 10 days it would be:

$$\$5,000 \times \sqrt{10} = 5,000 \times 3.1623 = 15,881.$$

So the value at risk to the 95% confidence level over 10 days would be:

$$1.645 \times \$15,881 = \$26,124$$

Obviously, the value at risk over ten days must be greater than over just one day as there could be a sequence of 10 days of 'bad luck'.

## 7. Sensitivity analysis

Sensitivity analysis examines how a decision might change if one **variable at a time** is changed. It is usually measured with respect to where a project or opportunity hits break-even point.

You might first have come across the principle in contribution analysis:

Unit cost card	\$	\$
Selling price		120
Material	30	
Labour	22	
Variable overhead	28	
Fixed overhead	<u>15</u>	
		<u>95</u>
Profit		<u>25</u>

Based on budgeted output of 10,000 units

$$\text{Budgeted fixed costs} = \$15 \times 10,000 = \$150,000$$

$$\text{Contribution per unit} = 120 - 30 - 22 - 18 = \$50$$

$$\text{Break even point} = \$150,000 / \$50 = 3,000 \text{ units.}$$

So, the actual output could fall from its budgeted level of 10,000 units to 3,000 before a loss starts to be made. The margin of safety (or sensitivity to volume) is 7,000 units or 70%.



Sensitivity is often used to assess net present value calculations. Look at this example:

### Example

Here is a project appraised at a discount rate of 10%. Sales volume is estimated at 1,000 units per year.

Time			\$ 10% discount factor	DCF \$
0	Cost	(130,000)	1	(130,000)
1 – 4	Sales	1,000@\$100 = \$100,000	3.17	317,000
1 – 4	Marginal costs	1,000@\$60 = (\$60,000)	3.17	(190,200)
4	Scrap	25,000	0.683	17,075
			NPV	<b>13,875</b>

The NPV is positive so the conventional advice would be to accept the project. However, the sensitivity of this recommendation to the various assumptions should be examined. This is done by seeing how far an assumption can change before the NPV = 0. Each assumption has to be assessed separately.

### Required

Examine the sensitivity of the solution to:

- (a) Initial cost
- (b) Selling price
- (c) Sales volume
- (d) Scrap value
- (e) Discount rate

### Solution

- (a) If the NPV is to be zero, the cost must rise by \$13,875 to extinguish the NPV.  
Sensitivity =  $13,875 / 130,000 = 10.7\%$
- (b) Selling price affects the revenue figure. If its PV of \$317,000 falls 13,875 then NPV = 0.  
Sensitivity =  $13,875 / 317,000 = 4.4\%$
- (c) Sales volume affects both revenue and marginal costs:  $317,000 - 190,200 = 126,800$   
Sensitivity =  $13,875 / 126,800 = 10.9\%$
- (d) The PV of the scrap value must fall by \$13,875 to produce a zero NPV.  
Sensitivity =  $13,875 / 17,075 = 82\%$
- (e) To work out the sensitivity to the discount rate, the IRR has to be calculated. So, NPV at 20%:

Time			\$20% discount factor	DCF \$
0	Cost	(130,000)	1	(130,000)
1 – 4	Sales	1,000@\$100 = \$100,000	2.59	259,000
1 – 4	Marginal costs	1,000@\$60 = (\$60,000)	2.59	(155,400)
4	Scrap	25,000	0.482	12,050
			NPV	<b>(14,350)</b>

By interpolation

$$\text{IRR} = 10 + (20 - 10) \times 13,875 / (13,875 + 14,350) = 14.9, \text{ or around } 15\%$$

So, the NPV is very sensitive to the selling price, which only needs to fall by about 4.4% before the project just breaks even. Not only is 4.4% small, but the selling price is probably difficult to estimate.

The cost could rise by about 10%. Not a large over-run, but at least cost is easier to predict and control than future flows.

Scrap value could fall by 82% - a large fall, but it will usually be difficult to predict the scrap amount.

The discount rate can rise from 10% to 15% (50%) and that would probably be judged unlikely.

### Note

- Sensitivity analysis allow only one variable to be changed at a time, whereas some changes might well be linked.
- It also say nothing about how likely a variable is to change. We have said that the project is very sensitive to selling price (4.4%), but if the selling prices had been already agreed for a four year contract, that 4.4% drop is unlikely to happen.

## 8. Risk adjusted discount rates

If a project's cash flows are perceived as being particularly either because they are simply difficult to predict or the project is inherently risky then a higher discount rate can be applied. This will more severely discount the more distant cash flows – which is just what you want because those are the flows that are least certain.

This subject is covered in more detail in a later chapter.

## 9. Certainty equivalents

Another way to account for future inflows being uncertain is to reduce them to their **certainty equivalent**, which can be defined as:

“the guaranteed amount of money that an individual would view as equally desirable as a risky asset.”

So, the flows being received at each of times 1, 2, 3 might be reduced to 90%, 75% and 60% of their ‘face values’ to account for further off flows being less certain.

There is no set way to reduce future flows. For example, for a particular project the reductions might be to 80%, 70% and 50%

The resulting cash flows would then be discounted the risk free discount rate. Do not reduce the flows to their certainty equivalence AND use a risk adjusted discount rate as that would be double counting.



## 10. Linear regression

Linear regression is a method of fitting the best possible straight line through a set of points.

In business, typically the line would connect points showing:

- Cost and volume
- Selling price and sales volume
- Hours worked and units produced

The predictions that might be made can be used by organisations to plan better and this will reduce risk. For example, if a company is thinking of reducing its selling price, it needs to have an idea of the volume of goods that will sell otherwise it risks not being able to meet demand and of alienating customers.

Linear regression will give constants which fit a line of the type:

$$y = ax + b$$

where:

y is the dependent variable (cost, hours, volume sold)

x is the independent variable (units made, selling price).

The constant 'a', for example, could be the additional cost for each additional unit made; 'b' would be the cost even if no units were made (the fixed cost).

However, be warned: linear regression will give the best line it can through any set of points.

For example, if you numbered the days in the year 1 – 365 and you noted the day each person was born and the amount of money they had in their bank account, linear regression would suggest the best relationship it could between these variables. Obviously there would not actually be a good relationship.

To test the relationship you must calculate the coefficient of correlation (r), or the coefficient of determination ( $r^2$ ). r can vary between:

$r = +1$ , meaning perfect positive correlation where all points lie on the line and as one variable increases, so does the other.

$r = -1$ , meaning perfect negative correlation where all points lie on the line and as one variable increases, the other decreases.

$r = 0$  means no correlation.

If  $r = 0.7$ ,  $r^2 = 0.49$  or about 50%. This means that 50% of the change in one variable is explained by the change in the other.



You should be aware of the following before you rely on any prediction based on linear regression:

- If  $r^2$  is low, then one variable is not well-associated with the other, so any predictions are liable to be poor.
- The more points (readings) the better: simply more evidence for the association.
- Extrapolation (predicting outside the range examined) is dangerous as we have no direct evidence of what happens in other regions. For example, costs might suddenly increase.
- Other known influences (such as inflation) should be removed before the analysis.
- Even good correlation does not prove cause and effect: both variables might have moved together under the influence of another variable.

## 11. Simulation modelling

Simulation attempts to model the possible results from a project by using ranges of values and random numbers to generate typical series of events. It is best carried out using a computer.

For example:

A company is considering a 6 year project, in volatile economic conditions. It is thought that growth or decline in the market from one year to the next will depend on the growth or decline that happened in the previous year:

If the market grows 10% in one year, there is a 75% chance that it will grow 10% the following year and a 25% chance that it will decline 10%. Similarly, decline of 10% in one year gives a 75% chance of 10% decline the next and a 25% chance of 10% growth.

To set up the simulation ranges of numbers are assigned to mimic the probabilities:

- If there is growth one year then for the next year: 00 – 75 = further growth; 76 – 99 = decline
- If there is a decline one year then for the next year: 00 – 75 = further decline; 76 – 99 growth.

Let's start with sales of 1000 units and assume that the previous year showed *growth*. Random numbers are then generated. For example: 63, 41, 5, 67, 98, 37, 74, 3, 12, 34, 95... and so on

Random number	63	41	85	67	98	37	74	83	12	95
Growth/decline +/- 10%	G	G	D	D	G	G	G	D	D	G
Sales	1100	1210	1089	980	1078	1186	1305	1175	1057	1163

This allows typical trading patterns to be examined and would allow the company to see what might happen if it had several years of decline in a row.





# Chapter 5

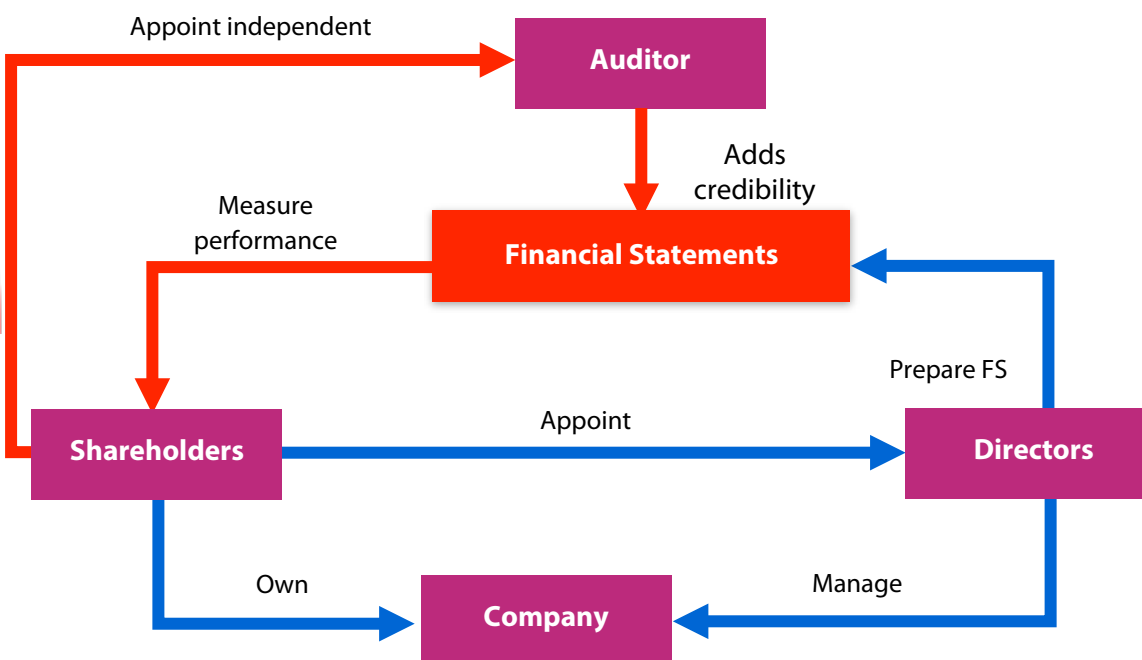
## CORPORATE GOVERNANCE

### 1. Why corporate governance is needed

Corporate governance is a system by which companies are directed and controlled.

The problem is that although the shareholders own companies, the day-to-day management and direction of companies is given to the Board of Directors. In large companies, many shareholders are relatively passive and the Board of Directors are given more or less free rein to make whatever decisions they wish.

Auditing was instituted so at least once a year, when the accounts were presented to the members of the company, the auditors would examine the accounts and give some expression of opinion to the members of the company as to whether the accounts were true and fair. Without that assurance the members of the company really would have a little idea as to whether or not the accounts were worth relying on. The auditors therefore examine the financial statements and this adds credibility to those statements, the shareholders have a much better idea of the performance of the directors and the company.



Note that shareholders appoint the independent auditors, they also appoint the directors. The problem is however that once directors were appointed, shareholders often didn't take much further interests in what the directors were doing. Scandals such as Enron, Worldcom in the early 2000's and perhaps banking problems in 2008 showed that this hands-off approach was entirely inadequate and additional safeguards have been instituted to try to ensure that directors act in the best interests of the members of the company.

## 2. Principles of corporate governance

The Organization of Economic Cooperation Development (OECD) has put forward some principles of corporate governance.

- Corporate governance frameworks should protect shareholders rights, ensuring fair treatment of all shareholders, particularly minority and foreign shareholders. For example all shareholders should have access to the same information.
- The corporate governance framework should also recognise the rights of all stakeholders, not just shareholders, and should encourage active cooperation between the entities and stakeholders in creating wealth, jobs and sustainability of financially sound entities.
- There should be disclosure and transparency.
- The corporate governance framework should ensure that timely accurate information is made available in all material matters.
- Responsibility of the board is also covered, and the corporate the corporate governance framework should ensure the **strategic** guidance of the entity, effective monitoring of management by the board and the board's accountability to the entity and their shareholders. In particular the board should set its own objectives, monitor its own performance and have its own performance assessed.

## 3. The UK Corporate Governance Code

The OECD principles are put into effect in a variety of ways in different countries. The UK Corporate Governance Code can be referred to as an example of best practice.

The code states that the purpose of corporate governance is to facilitate effective entrepreneurial and prudent management that can deliver long-term success of the company. It then goes on to list the main principles of the code:

### Main principles

- Leadership
- Effectiveness
- Accountability
- Remuneration
- Relations with shareholders

### Comply or explain

The code has no force in law and is enforced on listed companies through the Stock Exchange. Listed companies are expected "comply or explain" and this approach is the trademark of corporate governance in the UK. Listed companies have to state that they have complied with the code or else explain to shareholders why they haven't. This allows some flexibility and non-compliance might be acceptable in some circumstances.



## Leadership

- Every company should be headed by an effective board which is collectively responsible for the long-term success of the company.
- There should be a clear division ... between the running of the board and the executive responsibility for the running of the company's business. No one individual should have unfettered powers of decision. This means that the roles of CEO and chairman should not be performed by one person as that concentrates too much power in that person.
- The chairman is responsible for leadership of the board
- Non-executive directors (NEDs) must be appointed to the board and they should constructively challenge and help develop proposals on strategy. NEDs sit in at board meeting and have full voting rights, but do not have day-to day executive or managerial responsibility. Their function is to monitor, advise and warn the executive directors.

## Effectiveness

- The board should have an appropriate balance of skills, experience, independence and knowledge. In large companies NEDs should be at least 50% of the board; in small companies there should be at least 2 NEDs.
- New directors should be appointed by a Nomination Committee to ensure a formal, rigorous and transparent procedure for their appointment. The Nomination Committee consists of NEDs. This provision is to prevent directors appointing their friends and colleagues to the board and ensures that the best people for the job are considered and appointed.
- All directors should be able to allocate sufficient time to company business
- There should be induction on joining the board and a programme to update and refresh directors' skills and knowledge.
- The board should be supplied in a timely manner with necessary information
- The board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors.
- All directors should be submitted for re-election at regular intervals
- The board should present a balanced and u

## Accountability

- The board should present a balanced and understandable assessment of the company's position and prospects.
- The board is responsible for determining the ... significant risks ...and should maintain sound risk management and internal control systems.
- The board should establish formal and transparent arrangements for applying the corporate reporting, risk management and internal control principles, and for maintaining an appropriate relationship with the company's auditor. This means that an Audit Committee (NEDs again) should be established to liaise with both internal and external auditors. Before audit committees, the finance director liaised with auditors, but this was not satisfactory because the finance director was often the person responsible for accounting problems. Therefore auditors were often reporting problems to the person who caused them. The directors are responsible for establishing an internal control system and must review the need for internal audit.



## Remuneration

- Levels of remuneration should be sufficient to attract, retain and motivate directors of sufficient quality... but avoid paying more than is necessary.
- A significant proportion of executive directors' remuneration should be structured so as to link rewards to corporate and individual performance. In other words, profit related pay is encouraged. Directors should not receive high pay irrespective of company performance.
- There should be a formal and transparent procedure for developing policy on executive remuneration and for fixing the remuneration packages of individual directors. No director should be involved in deciding his or her own remuneration. This means that a Remuneration Committee (NEDs) should be formed to fix directors' remuneration.

Note the point that a significant proportion of executive directors' remuneration should be related to the profit or other success of the company. A long term relationship is really what's wanted so that directors cannot manipulate profits in the short term to manufacture bonuses for themselves.

Share option schemes can be very effective methods of remuneration. For example, if the current share price is \$8, offer share options at \$15, available after four years (the vesting period). If, after four years, the share price has risen above \$15, directors will exercise their options to buy at \$15 as this will produce a profit for them. If the share price were only \$12, the options would not be exercised. Therefore, the scheme encourages directors to act in a way that increases the long-term share price of the company – precisely what the shareholders would want then to do.

## Relations with shareholders

One of the problems with achieving good corporate was encouraging shareholders to take an active interest in the company. Too often they did not fully participate at AGMs and would wave through motions. This passive attitude might well have been encouraged by directors to move power towards them and away from members.

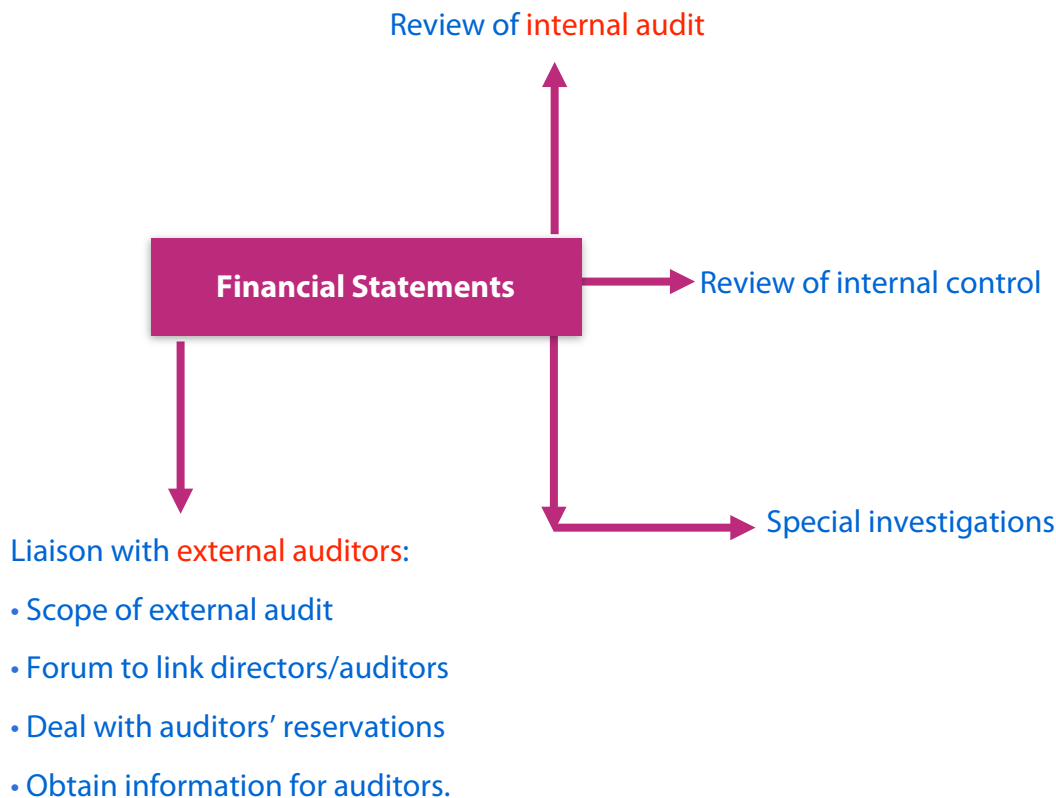
### The code therefore specifies:

- There should be a dialogue with shareholders based on the mutual understanding of objectives. The board as a whole has responsibility for ensuring that a satisfactory dialogue with shareholders takes place.
- The board should use the AGM to communicate with investors and to encourage their participation.



## 4. The role of the audit committee

The audit committee is now very important part of corporate governance.



The committee should be dominated by non-executive directors. The functions are as follows:

- They will review the work of internal audit. Companies don't have to be an internal audit department, but corporate governance rules now stated management should keep the need for internal audit on the review.
- The audit committee will review the system of internal control. Corporate governance now imposes on management the requirement that they implement a system of internal control.
- From time to time the audit committee may launch special investigations. For example, if a fraud had been discovered within the organization the audit committee may ask for a report on how it happened and how to prevent it in the future.
- Liaison with external auditors. It used to be that external auditors would communicate almost exclusively with the finance director, but of course the finance director may not be sufficiently independent of the finance function and the system of internal control. Now, the audit committee will set the scope for the external audit. They act as a forum to link directors and auditors. Auditors will typically write to the audit committee about any problems they may be having on the audit or obtaining all the information they require. If the auditors are worried in some way about the financial statements they will raise those concerns with the audit committee.
- If the auditors can't find information in any other way and feel perhaps they are being obstructed, they can go to the audit committee and explain the problem and the audit committee can try to investigate on their behalf.
- Liaise on the process of appointing auditors and setting their fees. (Note that the external auditors are appointed by members in general meeting, but the audit committee is likely to make recommendations.)





# Chapter 6

## INTERNAL CONTROL AND AUDITING

### 1. Introduction to internal control

#### Internal control:

'The management system of controls, financial and otherwise, established in order to provide reasonable assurance of: (a) effective and efficient operation (b) internal financial control (c) compliance with laws and regulations'

(CIMA Official Terminology, 2005)

Examples of the three areas of internal control mentioned in this definition are:

Internal control area	Examples
Effective and efficient operation	<ul style="list-style-type: none"> <li>Enough inventory to meet production requirements</li> <li>Low wastage</li> <li>Full use of machinery through clever scheduling</li> </ul>
Internal financial control	<ul style="list-style-type: none"> <li>Safeguarding assets</li> <li>Collecting receivables on time</li> <li>Paying suppliers and employees the correct amounts</li> </ul>
Compliance with laws and regulations	<ul style="list-style-type: none"> <li>Ensuring working time and minimum wage laws are not broken</li> <li>Paying the correct amount of tax on time</li> <li>Ensuring health and safety laws are complied with</li> </ul>

Note that the term encompasses more than just financial controls - though it is financial controls that auditors will concentrate on.



## 2. The elements of internal control

International Standards on Auditing 315

- **The control environment.** This refers to the culture of the organisation: Is good internal control valued and encouraged?
- **The risk assessment process.** Where is the organisation vulnerable? For example, a jewellery shop will need very good control over its inventory.
- **The information system.** How does management receive information that might indicate that internal control is failing? For example, comparing budgets to actual results might indicate a problem.
- **The control activities:** For example authorisation, reconciliations, comparisons, physical controls, numerical sequence control
- **Monitoring:** is the internal control system being kept up to date with respect to business developments? Is it operating properly?

You might remember the front face of the COSO cube on enterprise risk management. That set out how risks should be managed. It is worth repeating that here to see the similarities between the COC elements of risk management and the ISA elements of internal control.

- **Internal environment**

This can be regarded as the outlook and culture of the organisation, including its enthusiasm for risk management and its risk appetite.

For example, some organisations are a bit happy-go-lucky when it comes to risk management whereas others are extremely strict and want things to be done by the book.

- **Objective setting**

Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

The objectives of a manufacturing department is to make the right goods to the right quality and at the right cost. The department cannot be managed without objectives and performance measurement.

The objectives the accounts receivable department will be to achieve a certain collection period and to minimise bad debts. Again, objectives and targets are needed to manage and appraise this process.

Similarly, with regard to minimum wages, unless those are defined and compared to actual wages, no control is possible.

- **Event identification**

There are internal and external events (both positive and negative) which affect the achievement of an entity's objectives and must be identified. For example, there must be a way of accounting for waste and quality control failures.



## ● Risk assessment

Risks must be analysed to consider their likelihood and impact as a basis for determining how they should be managed. The results of this exercise should be noted on the risk register and the assurance mapping document.

## ● Risk response

Management selects risk response(s) to transfer, avoid, reduce or accept risk (TARA).

The aim is to align risks with the entity's **risk tolerance** and risk appetite. Risk tolerance is the acceptable variation in outcome compared to an original objective. In setting risk tolerance, management considers the relative importance of the related objective. So, if an objective is particularly important, risk tolerances might be higher to recognise that achieving something really worthwhile is worth accepting more risk.

## ● Control activities

Policies, procedures and control methods help to ensure risk responses are properly carried out. Examples of control activities include authorisation of transactions, reconciliations, segregation of duties (splitting a transaction so that several people are involved), physical controls (such as locking away valuable inventory), the comparison of actual results to budgets. IT controls can also be very important.

## ● Information and communication

Information that monitors or identifies risks must be identified, recorded and communicated quickly enough and in a way that lets people carry out their responsibilities by making decisions. For example, if a product's sales are lower than expected, this information must be available quickly enough to change prices, alter the advertising campaign – or to withdraw the product.

## ● Monitoring

The entire process must be monitored and modifications made as necessary, to improve current methodologies and to adapt to emerging risks, so that the system stays relevant. For example, if the company starts to trade on the internet a whole new set of risks arises. For example, their system could be 'hacked'. More on this in a later chapter.



### 3. Responsibilities

The UK Corporate Governance Code states that it is the responsibility of the board of directors to establish procedures to manage risk, oversee the internal control framework and determine the nature and extent of the principle risks that the company is willing to take in order to achieve its long-term strategic objectives.

It is then the responsibility of the audit committee (a sub-committee of the board) to review the company's internal financial controls and internal control and risk management systems unless expressly addressed by a separate board risk committee composed of non-executive directors or the board itself.

The audit committee should review the effectiveness of the company's internal audit function or, if there isn't one considering annually whether one is needed and making a recommendation to the board.

The audit committee must also review the effectiveness of the external audit process.

### 4. Internal control systems

Most auditing relies on testing the system of internal control. This is the system put in place to prevent or detect errors. Typical controls are:

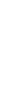
- Segregation of duties: split up the stages of a transaction so that one person doesn't carry out every step. This helps to stop fraud and also means that several minds are involved in ensuring the transaction is correct.
- Physical: for example, lock cash and inventory away.
- Authorisation and approval: for example, overtime claims are signed by managers as approval.
- Management and supervision: managers and supervisors keep an eye on what's going on.
- Organisation: for example, ensuring that the sales team can't decide on sales prices to boost demand and their commissions.
- Arithmetic and accounting: reperform calculations. Carry out reconciliations.

Internal control systems should be set out in a procedures manual and internal auditors will assess:

- Are the procedures adequate?
- Are the procedures being carried out as they should be?

Examples of poor internal control include:

- Not cancelling suppliers invoices when posted/paid (they could go round the system again).
- Employees self-certifying time sheets and expense claim forms
- Ability of junior staff to write off debts (or to carry out other journal entries).
- Not ensuring that cash receipts are promptly banked
- Not establishing credit limits for customers and not following up slow payers
- Not approving orders for material so that too much of the wrong type can be ordered



## 5. External and internal audit

### External audit:

'A periodic examination of the books of account and records of an entity carried out by an independent third party (the auditor), to ensure that they have been properly maintained, are accurate and comply with established concepts, principles, accounting standards, legal requirements and give a true and fair view of the financial state of the entity.'

(CIMA's Management Accounting Official Terminology)

There is a statutory requirement for all but the smallest company's to have an external audit each year. This reports to the members (shareholders) on whether or not the financial statements (in the opinion of the auditor) show a 'true and fair' view.

### Internal audit:

'An independent appraisal activity established within an organisation as a service to it. It is a control which functions by examining and evaluating the adequacy and effectiveness of other controls; a management tool which analyses the effectiveness of all parts of an entity's operations and management.'

(CIMA's Management Accounting Official Terminology)

CIMA members and the P3 exam are primarily focussed on internal audit.

Whereas external auditors are employed by an independent firm (such as one of the 'big four: PWC, KPMG, EY and Deloitte) internal auditors (IA) are usually employees of the company (though the process of internal audit can be outsourced) and this can interfere with the independence and of the internal audit function. IA might fall under the control of the finance director and then IA staff would potentially have to report problems with financial internal control to the director who has prime responsibility for internal control. It is easy to see how the finance director might like problems to be minimised or 'hushed up'. It is therefore strongly recommended that IA reports to the audit committee, chief executive officer and board of directors rather than to the finance director.



CIMA guidance for internal auditors is:

- The aims of internal audit should be agreed by the board.
- Should cover all controls, not just accounting.
- There should be full access to people and documents.
- There should be clear access to the CEO, chairman and the audit committee.
- Internal audit should report to a senior director or the audit committee.
- Internal audit should be independent of executive management so as to maintain their independence.
- Best practice for auditing methodologies and the latest auditing standards should be used.
- Internal audit should be consulted on all major business changes so that suitable controls can be implemented promptly.
- The internal auditors should have no operational involvement elsewhere in the organisation.
- There must be clear communication of findings.
- The performance of internal audit should be regularly assessed.

## 6. Internal audit – types of assignment

- Transactions audit: tracing transactions through the system, often from start to finish, to see if they are treated correctly.
- Systems audit: an information technology or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure.
- Risk-based audits: an internal audit which is primarily focused on the inherent risk involved in the activities or system and provide assurance that risk is being managed by the organisation to the defined risk appetite level.
- Accounting systems audit: ensuring, for example, that the proper accounting controls are being applied consistently.
- Operational audits: a systematic review of effectiveness, efficiency and economy of operation. For example, examining how customer complaints are dealt with.
- Value for money and best value. Usually associated with public or non-profit organisations. Its purpose is to assess the effectiveness and efficiency of its use of public funds.
- Management audits: analysis and assessment of competencies, abilities and capabilities of a company's management in order to evaluate their effectiveness, especially regarding the strategic objectives and the implementation of the policies of the business.
- Social and environmental audits: A social and environmental audit looks at factors such as a company's record of charitable giving, volunteer activity, energy use, recycling waste, diversity in recruitment, non-discrimination in appointments, the standard of the work environment, workers' remuneration to evaluate the social and environmental impact the company is having.
- Special assignments such as investigating a case of fraud.
- Assisting the external auditors.

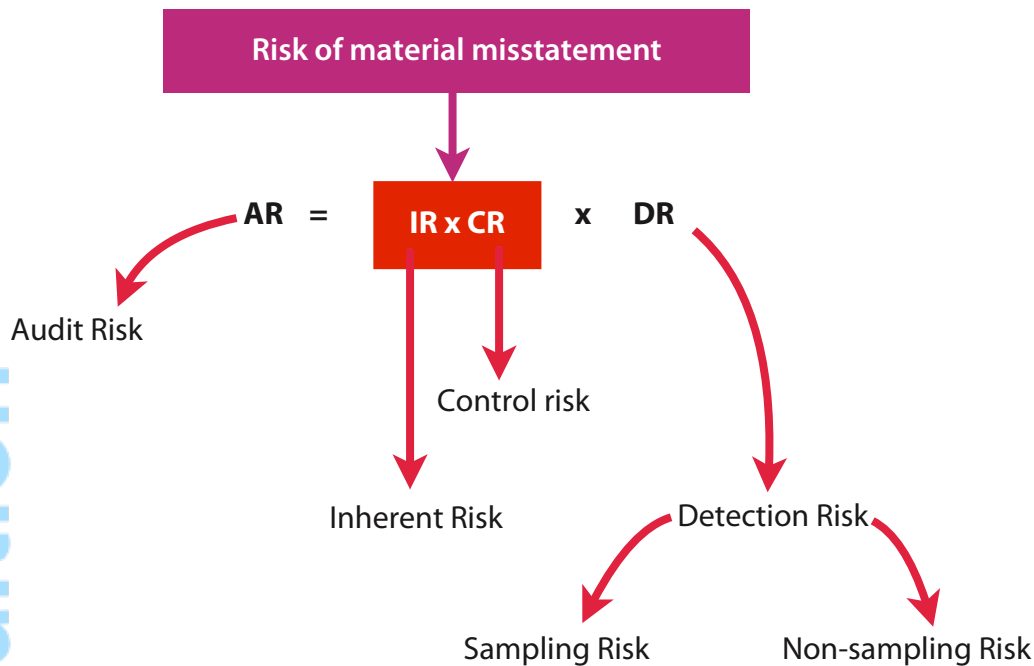


## 7. Comparison of internal and external audit

	Internal audit	External audit
Reports to	Management – must have a clear route to the board though day-to-day reporting to the audit committee.	Shareholders
Appointed by	Management	Shareholders
Power from	Management	Statute – allows external auditors to insist on seeing all documents and to be given full explanations.
Employed by	Company (unless outsourced)	External firm
Coverage	All categories of risk and investigation	Financial statements: true and fair view
Responsibility for improving the organisation	A major function of internal audit	Will report to management on internal control weaknesses



## 8. The audit risk model



The audit risk model sets out the current, risk-based, approach to auditing.

Audit risk is the risk that the auditor comes to a wrong conclusion about a figure in the financial statements or the accounting system. For example, the auditor, whether internal or external, concludes that an amount is correct when, in fact, it is wrong.

**For that to happen, three problems must have occurred:**

- **Inherent risk:** this is the risk that an error is made in the first place before the application of any controls or checks. Inherent risk is increased by factors such as:
  - ▶ Inexperienced staff
  - ▶ Time pressure
  - ▶ Complex transactions
  - ▶ Figures requiring a high degree of estimation
  - ▶ Pressure to perform well eg to make results look good.
  - ▶ **Control risk:** this is the risk that the organisations system of internal control does not prevent or detect the error. For example, a junior employee might have committed an error (inherent risk), but good supervision and checking of that person's work should detect and correct the error.

If both of these occur, then a wrong figure is in the financial statements or in the accounting records.

- **Detection risk:** this is the last line of defence and this refers to work the auditor does. If the auditor performs a lot of work, detection risk will be low as there is a good chance that the audit work detects the problem. If the auditor does relatively little work, then the chance of picking up an error will be low.

Auditors can't alter inherent risk or control risk in the short term (though they should certainly be able to influence control risk in the long term). Therefore, to keep the audit risk low (and this is essential), if the auditor perceives high inherent and control risk, a large amount of

audit work will have to be performed. If, however, the auditor perceives inherent and control risk to be low, the auditor will perform much less audit work yet still achieve a reasonable degree of assurance about the figures in the accounting system.

Detection risk depends on:

- ▶ Sampling risk – if a sample is too small then errors might not be found. This risk is decreased by increasing sample sizes.
- ▶ Non-sampling risk – typically because the auditors are too inexperienced, badly supervised and their work poorly reviewed. Samples could be 100% but if the auditor didn't know what he or she was looking for detection risk will be very high.

## 9. Audit planning

The first step in any audit is to plan: what are the main risks? How will they be addressed? How many auditors do we need and with what experience? How long will it take? How many locations do we need to visit?

Risk can be assessed by:

Knowledge of the business. For example, a jewellery business will have high risk in inventory (small, high-valued items).

- Talking to staff. For example, they might tell the auditor of an accounting problems or that the new IT system was giving problems.
- Analytical procedures or analytical review. Compare this period's results with last period's results and with budgets. Analytical reviews are quick to carry out and can be used to highlight areas where something might have gone wrong and therefore where risk is high. For example, if receivables collection periods have increased from 34 days to 56 days the auditors need to know why. Is it a deliberate change to the credit terms? Are there more export customers where the transportation of the goods can take time so that payment is delayed? Has the credit control department become sloppy? Is it an error? Is there a large unrecoverable amount that should perhaps be written off? Another example would be if the gross profit percentage had risen from 30% to 40%. How can that happen in a competitive market? Perhaps the company had a technical breakthrough so that it could make and sell a uniquely good product? However, it might be more likely that an accounting error or change in accounting policy is the cause. Remember, supermarkets get quite excited if their like for like sales rise by just a few percentage points over a year so a GP% jump from 30% to 40% is remarkable..



## 10. Collecting audit evidence

Auditors collect evidence in the following ways (AEIOU):

- **Analytical procedures** – ratios and comparisons as explained above.
- **Enquiry and confirmation:** for example, ask employees how they carry out certain operations. Write to customers and ask how much they think they owe.
- **Inspection:** for example, inspect orders to ensure they have been properly authorised
- **Observation:** for example, watch operations in the receiving bay to ensure that personnel count and inspect the goods delivered.
- **Recalculation and reperformance.** For example, redo a bank reconciliation to ensure that it was carried out correctly.

## 11. Computer assisted audit techniques

### 11.1. Introduction

Even very small businesses will usually maintain their computer records on computer. There are many advantages to this, not least that trial balances will usually balance and control accounts will reconcile to the underlying detailed records. However, the absence of as many hand-written data and documents data can make auditing more difficult. For example, it can be difficult to test whether a computer is carrying out a procedure correctly and it can be more difficult to 'see' and examine the information and records than in a manual system.

Computer Assisted Audit Techniques (CAAT) have been developed to assist the auditor when the client maintains computerised records.

### 11.2. Types of CAAT – audit software

Audit software (or audit programs) is software developed and used by auditors. Audit software allows clients' accounting data files to be read and examined.



The processes carried out by the auditor's software commonly include:

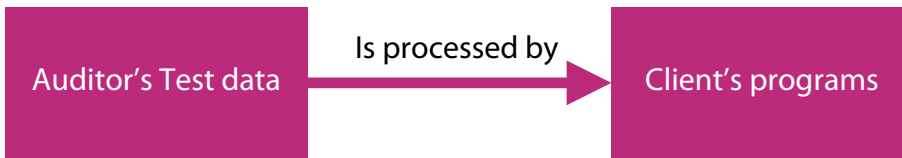
- Adding up the records. For example, inventory values and receivables balances. The totals are the amounts that should appear in the statement of financial position.
- Performing calculations for analytical reviews.
- Identifying and printing details of unusual items for further investigation, such as credit balances on a receivables ledger or negative inventory balances.
- Picking samples. For example, that audit software can be programmed to create a stratified sample or a pure random sample.
- Picking all items with particular characteristics, such as all sales orders approved by a certain employee.



Once it is set up, audit software can quickly, efficiently and economically examine every item on a data file. This which would often be difficult or impossible if attempted manually. It can greatly speed up audit completion and reduce costs.

### 11.1.Types of CAAT – test data

Test data is auditor's data that is operated on by client's program. It is used to test the workings and resilience of programs.



The results produced by client programs are compared with predictions of what should happen and any discrepancies are investigated.

#### Test data is designed to:

- Test that calculations are carried out correctly by client software. For example, enter time sheet data of 50 hours worked and ensure that the correct wages and tax are calculated.
- Test that programmed controls and procedures are carried out correctly. For example, if a client's system should reject orders from customer over their credit limit, test that such orders are indeed rejected by entering an order that should be rejected. Another example of a programmed control would be testing that only staff members who are allocated certain privileges can log-on and change someone's salary: log-on with what should be inadequate rights and ensure that you cannot change a salary.
- Test how resilient software is against input errors. For example, test what happens if an account number is entered incorrectly, or a negative amount of stock id ordered, or an impossible date is entered.

Test data might be the only way in which certain controls can be verified. For example, a company web-site might properly reject an order from a customer, but there might be no permanent record available to the auditors to verify that this control is happening.

### 11.1.Problems with CAAT techniques

- Technical/set-up problems. Initially, additional time and technical expertise will be needed to set up audit software and test data properly. The time and expenses of this should be repaid in subsequent years.
- Clients or departments can be reluctant to let auditors interfere with their computer records. This is more of a problem with test data where deliberately false transactions are processed to test the system. The normal way round this is for the auditor to use a copy of the system and to process their test data against that. This technique is known as 'dead' test data. There is a risk, of course, that the programs being used are different to the copies being used by the auditor.



## 12. The internal audit report

At the end of the audit process, internal auditors will issue a report that will detail:

- Deficiencies in the internal control system's design
- Incidents where the internal control system was not complied with
- Errors discovered

Often the reports will be in the format:

Details about the nature of the internal control deficiency and departures from the specified internal control procedures	The possible effects of these deficiencies and departures	Suggestions for fixing the problems
---	---	-------------------------------------

## 13. Responsibilities, status and outsourcing

### 13.1. Responsibilities for internal control

Note that directors are responsible for:

- Maintaining sound risk management and internal control systems
- Setting the control environment (a culture where there is an appreciation of the benefits and importance of controls, internal control procedures and their operation)
- The effectiveness of these elements should be regularly reviewed.
- Keeping the needs for internal audit under regular review
- Listed companies must report on internal control in their annual reports.

### 13.1. Status and qualifications

**Internal auditors should be:**

- Qualified
- Experienced
- Independent
- Professional

Although ultimately they report to the board this will often be through the audit committee. Even then, because of the employer/employee relationship it might be difficult for internal auditors to criticise internal controls set up by the finance director.



### 13.1. Outsourcing internal audit

It is increasingly common for the internal audit function to be outsourced (ie internal audit functions are externally supplied). Advantages and disadvantages of this are as follows:

Advantages	Disadvantages
No recruitment, staffing or training worries	Less knowledge and expertise about the business
Specialist services will be available from large external suppliers that might be difficult to provide in-house eg forensic investigations	Cost – external providers will charge quite high hourly rates.
Flexibility to carry out special investigations that are urgent	There can be ethical complications if external auditors are used in an internal audit function
Quicker to set up initially	
Appropriate amounts of time can be spent. A company might not be large enough to keep an internal audit team fully employed (and a team is needed to provide mutual strength).	
Greater independence	

## 14. Fraud

### 14.1. Introduction

Fraud is an intentional act involving deception to gain unjust or illegal advantage.

There are two types:

- Fraudulent financial reporting. For example, overstating profits to generate high directors' bonuses, boost the share price or to achieve a good sale price for the company.
- Misappropriation of assets. For example theft of cash or inventory.

Managers and those charged with governance are responsible for the prevention or detection of fraud. Auditors should always be aware of an organisation's susceptibility to fraud.

Fraud can be difficult to detect because:

- It is often carried out by repeatedly misappropriating small amounts that escape individual scrutiny.
- Fraudsters take steps to conceal their actions, for example, forging documents. These can be very difficult to identify.



## 14.1. The pre-conditions for fraud:

Three conditions or risk factors are necessary for fraud to be committed:

- Incentive
- Opportunity
- Attitude/dishonesty

Risk factor	Examples relating to fraudulent financial reporting	Examples relating to the misappropriation of assets.
<b>Incentive</b>	<ul style="list-style-type: none"> <li>● Pressure from shareholders to perform</li> <li>● Fear of losing job</li> <li>● Incentives related to performance</li> </ul>	<ul style="list-style-type: none"> <li>● Personal financial pressure</li> <li>● Greed</li> <li>● Dislike of the employer (I'll get my own back!)</li> </ul>
<b>Opportunity</b>	<ul style="list-style-type: none"> <li>● Poor internal control</li> <li>● Poor corporate governance eg a dominant chief executive who is also chairman</li> <li>● Results dependent on many estimates and a high degree of judgement</li> </ul>	<ul style="list-style-type: none"> <li>● Poor internal control</li> <li>● High-value portable inventory</li> <li>● Cash-based business</li> <li>● Poor supervision</li> </ul>
<b>Attitude</b>	<ul style="list-style-type: none"> <li>● Poor ethics</li> <li>● Poor morale</li> <li>● Excessively aggressive targets</li> </ul>	<ul style="list-style-type: none"> <li>● Poor ethics</li> <li>● Dislike of the employer</li> <li>● Other employees' behaviour (and you become convinced that the 'fiddle' is normal and therefore acceptable)</li> </ul>

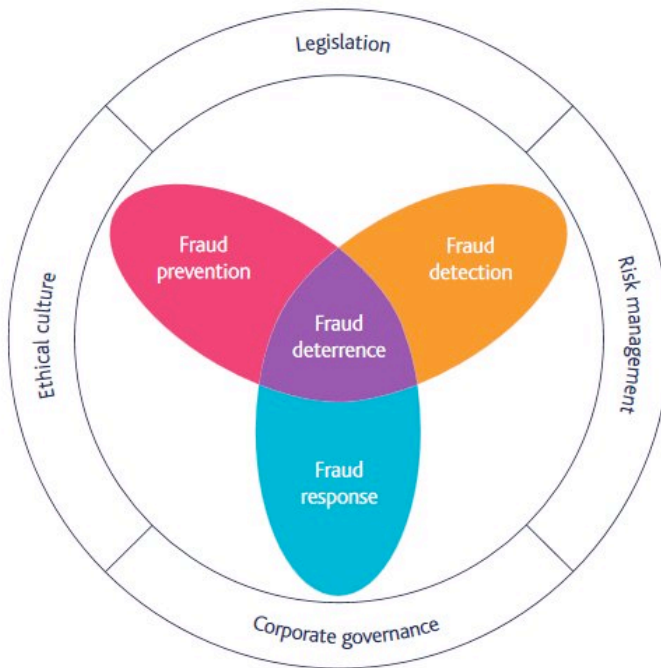


## 14.1. An anti-fraud strategy

An anti-fraud strategy has three elements:

- prevention
- detection
- response

CIMA shows that these interrelate as follows:



(Fraud risk management: a guide to good practice, CIMA)

Deterrence is the result of prevention (too difficult to get to the inventory to steal it), detection (you will be subject to random searches as you leave the factory), response (you will definitely be prosecuted).

Surrounding these specific anti-fraud strategies there are:

- **Legislation:** for example, what types of actions (such as insider trading) are illegal?
- **Risk management:** an awareness by the organisations senior managers and directors of where the main dangers of fraud lie and then suitable controls being put in place.
- **Corporate governance.** For example, non-executive directors providing independent advice about behaviour. Audit committee being available to support internal audit and whistleblowers.
- **Ethical culture:** for example, making it clear that 'shady' practices are wrong and will not be tolerated by the company. Training in ethical behaviour will be important





# Chapter 7

## ETHICAL CONSIDERATIONS

### 1. Ethics

#### 1.1. Introduction

**Ethics** is concerned with distinguishing between good and evil, between right and wrong human actions, and between virtuous and non-virtuous characteristics of people and organisations, and the rules and principles that ought to govern behaviour.

There is, of course, a range of views on what constitutes ethical behaviour. Different individuals and people from different cultural backgrounds might disagree on what constitutes acceptable behaviour in business. For example, in Japan punctuality is extremely important and to be late for a meeting is simply unacceptable. People from some other countries assume that a meeting starting at 2pm probably won't start until 3pm and punctuality is almost seen as a peculiarity. Ethical judgements also differ on matters such as:

- Health and safety
- Commissions/backhanders
- Conflict of interest
- Intellectual property rights

We do not need to get into how or why certain actions are considered ethical or unethical, but if investors, governments and customers or employees think, for whatever reason, that a company has acted unethically then the company will be damaged because of reputational loss, regulatory and legal sanctions, and also the fear that if one instance of unethical behaviour has been discovered how many other instances might still be hidden.

### 2. The importance of ethics in business

As mentioned above, different stakeholders are likely to have different ethical views. For example, on a crowded train some standard class passengers might see nothing unethical about sitting in first class ("I've bought a ticket I should have a seat"); some other passengers and managers of the train company might see this as unethical ("You can buy extra comfort if you want to"). Some shareholders might have ethical objections to their company taking part in arms manufacturing whilst directors and employees might have no ethical objections.

Perhaps what is most important is that stakeholders are informed about a company's ethical position on a number of issues so that there is openness and that everyone understands the company's ethical stance. **Corporate codes of ethics** can help to achieve this and therefore manage risks arising from unethical behaviour. These are documents issued to employees that attempt to establish ethical rules or guidelines so that employees know how to behave if, for example, offered a bribe by a supplier or they see a machine in a dangerous condition, or they are considering whom promote.



Often these guidelines are made available to outside stakeholders to advertise the company's ethical stance. For example, the Coca Cola ethical guide can be found at:

[http://assets.coca-colacompany.com/45/59/f85d53a84ec597f74c754003450c/COBC\\_English.pdf](http://assets.coca-colacompany.com/45/59/f85d53a84ec597f74c754003450c/COBC_English.pdf)

Here is a short extract from the section dealing with treatment of customers, suppliers and consumers:

"Always deal fairly with customers, suppliers and consumers, treating them honestly and with respect:

- Do not engage in unfair, deceptive or misleading practices.
- Always present Company products in an honest and forthright manner.
- Do not offer, promise or provide anything to a customer or supplier in exchange for an inappropriate advantage for the Company."

Employee training and full support from the top of the organisation is needed if an ethical culture is to be adopted. There is little point in handing employees the organisation's Ethical Guide if they are not taught how to apply it or if directors and managers ignore it.

Even if stakeholder disagrees about what appropriate ethics are, the importance of an organisation being ethical can be linked to its profitability or its financial viability. Organisations might obtain advantages by being unethical (for example to encourage sales a pharmaceutical company could conceal a drug's side effects) but most ethical breaches are discovered and then huge damage is done both financially and reputationally. Good ethics therefore:

- Reduces the risk for shareholders.
- Lower risk means that capital can be raised more cheaply (the cost of capital and risk are linked).
- Goodwill towards the company is increased – improving sales.
- Regulatory compliance is easier to achieve, reducing the cost of damages and fines.
- Good candidates are attracted to companies with good reputations
- Joint ventures are easier if the company has a good reputation

### 3. Examples of ethical dilemmas.

- Moving a factory to another town or country: many existing employees will lose their jobs.
- Building a new factory: local roads will become busier and there might be more pollution.
- Extracting resources from the earth: the potential for environmental damage.
- Insisting that the cost of bought in products is reduced: potential exploitation of labour.
- Ignoring health and safety rules, minimum pay and maximum working hours rules: exploitation of labour.
- Gathering and swapping information about customers: loss of customer privacy.
- Careless custody of customer data: potential fraud attacks on customers.
- Poor software testing: inconvenience and damage to customers.
- Not paying suppliers promptly: damage to suppliers and their workforces.
- Poor testing of products: potential damage to customers.



## 4. CIMA's ethical guidelines

The CIMA Code of Ethics for Professional Accountants is based on The CIMA Code of Ethics is based on the IFAC Handbook of the Code of Ethics for Professional Accountants, of the International Ethics Standards Board of Accountants (IESBA). The Code can be regarded as an overarching set of ethical principles for CIMA students and members.

The Code of Ethics sets out certain fundamental principles about how its members should behave. It also recognises how its members could be subject to certain threats which would compromise their behaviour and suggests ways in which members can safeguard themselves against the operation of those threats.

The guide applies to all members of CIMA working in industry, commerce and public practice. It also applies to all CIMA students. Note that its operation is not restricted to auditors and covers CIMA members working in industry and commerce. The fundamental ethical principles are:

- **Integrity:** Be straightforward and honest in all professional work. Stand up for what you believe to be right and do not be pressurised into accepting something you know to be wrong. Do not 'turn a blind eye' if you think something is wrong or unethical.
- **Objectivity:** Do not allow bias, self-interest or conflicts of interest to influence professional judgements and conclusions.
- **Professional competence and due care:** Carry out work to proper standards; don't skimp; keep up to date with changes in legislation, methodology and regulations.
- **Confidentiality:** Do not disclose information received through professional work without permission or if there is a legal duty or right to disclose it.
- **Professional behaviour:** Comply with laws and regulations and do not act in a way that brings CIMA or the wider accountancy profession into disrepute.

Compliance with the ethical guidelines is continually threatened. For example, integrity and objectivity can be threatened by personal relationships which could mean that an accountant does not want to report errors made by colleagues. Accountants have to ensure that threats are reduced to acceptable levels.



## 5. Approach to ethical dilemmas

- Identify threats/potential problems
- Evaluate their significance
- Raise internally (eg manager, audit committee, ethics committee)
- Raise externally (eg CIMA, legal advisers, whistle blow)
- Remove your self from the situation



# Chapter 8

## CYBER RISKS

### 1. What is 'cyber risk'?

Cyber risk can be defined as any risk of financial loss, disruption or damage to the reputation of an organisation by some sort of failure of its information technology systems.

(The Institute of Risk Management)

Cyber risk can arise from:

- Deliberate breaches of security
- Accidental breaches of security
- Operational causes (such as physical breakdown, wrong data or flawed software being used).

Before we address specific risks and how they might be defended against it is worth looking first briefly at how organisations use computers and the various physical arrangements that IT systems can adopt.

### 2. The uses of information in a business

#### 2.1. Levels of management and their use of IT

Information technology has to support staff at all levels, but there are quite different information needs at different levels:



**Corporate/strategic level needs information which tends to be:**

- Forward-looking (at this high level of management, people should be planning for the future) and historical.
- Often has to deal with estimates
- Often not to the last degree of accuracy – perhaps dealing with the nearest \$1m.
- Outward-looking (how are competitors, countries economies and technologies developing?)
- Supports unstructured decision-making ie where there is no definitive way at arriving at the right answer. For example, should we open an operation in Brazil?
- Non-routine/ad hoc.

Operational control level deals with information which tends to be:

- Historical
- Routine
- Internal
- Very accurate
- Supports structured decisions such as don't accept an order if over a customer's credit limit)

Information for business and management control (in the middle) is:

- Moderately forward looking (for example, will the division reach this year's budget?)
- Semi-structured decisions (such as should we manufacture more stock?)
- Reasonably accurate.

Disruption of IT at any level can be devastating for a company. For example, the routine processing of sales orders, whether they are received via the company's internet site or through the post is part of the operational level. Obviously things could go wrong in either case, but the opportunities for chaos are much greater in the Internet system because once a company is connected to the Internet, the Internet and all its users, many of whom might be malicious, are connected to the company.

As you go up through the hierarchy, into the corporate and strategic level, the information is more likely to deal with the company's future plans. So if board minutes are held on computer and these become available to outsiders and competitors (through industrial espionage) very serious long-term damage can be inflicted on the company.

Perhaps, the specifications of designs, chemical formulae for pharmaceuticals in clinical trials, databases about suppliers are held in the middle, managerial level. Any leakage of that information (industrial espionage again) can again seriously impact an organisation's profitability and its chance of survival.



## 3. Physical arrangements for IT systems

### 3.1. Networks

Only the very smallest of businesses will have stand-alone computers ie computers not connected to other computers. Even in small businesses employees need to share data and very soon after personal computers were invented networks of computers were introduced.

There are two main types:

- **Local area network (LAN):** Here the network extends over only a relatively small area, such as an office, a university campus or a hospital. The small area means that these networks use specially installed wiring to connect the machines.
- **Wide area networks (WAN):** Here the network can extend between several cities and countries. Each office would have its LAN, but that connects to LANs in other offices and countries using commercial, public communications systems. At one time this would have been done by the organisation leasing telephone lines for their private use to transmit data from office to office. However, this is expensive and inflexible and the common system now used is known as a virtual private network (VPN).

### 3.1. Network layers

Most client-server networks comprise of three tiers:

- The presentation tier: this is what you see on your computer screen: information, boxes in which to input data, buttons to click on, drop-down menus to choose from. This will be on the client machine.
- Application tier: this tier, sometimes known as the logic or business logic tier, is where processing takes place. It can be on the client machine or in the cloud. (see later).
- Data tier: where the data is stored, typically a database. It will normally be on the server machine or in the cloud.

So, if you are posting a supplier's invoice, you will enter the account number into the presentation tier, the application will access the data tier, fetch the customer name and this will be shown to you in the presentation tier. You will enter the amount and nominal code in the presentation tier, the application tier might split out VAT automatically, then post the amounts to the appropriate files in the data tier.

Security problems can happen at any tier. For example:

- A presentation tier might be hijacked so that it looks like, for example, your bank's web-page, but it is actually a page mocked up to look official (phishing)
- The application tier might be changed to calculate invoices incorrectly.
- The data tier might be accessed so that confidential data is stolen or records altered.



### 3.1. Virtual private networks (VPNs)

**VPN's** allow data to be transmitted securely over the internet between any two locations. Information will pass over many different circuits and connections but the system gives the impression that you are operating over a dedicated, private communications link: hence the name: virtual private network. For example, an employee working from home or a hotel can access the company system as though being in the office. Because data is being transmitted over public systems it is particularly vulnerable to interception and it is very important that adequate security measures are in place to safeguard the data.

There are three essential steps in the security measures:

- (1) **Access control and authentication** – this ensures that unauthorized users do not access the system. Typically this will be accomplished through a log-in procedure.
- (2) **Confidentiality** – this ensures that data cannot be intercepted and read by a third party whilst being transmitted. This is achieved using encryption.
- (3) **Data integrity** – this ensures that the data has not been altered or distorted whilst in transit. To ensure this, the message could have special check digits added to ensure that the data complies with a mathematical rule.

### 3.2. Centralised and decentralised (distributed) architectures

Consider an office local area network. There are three main ways in which the data and processing can be arranged: centralised, decentralised (distributed) and hybrid.

#### Centralised systems.

In these systems there is a powerful central computer which holds the data and which carries out the processing.

The main advantages of such systems are:

- Security: all data can be stored in a secure data centre so that, for example, access to the data and back-up routines are easier to control.
- One copy of the data: all users see the same version of the data.
- Lower capital and operational costs: minimal hardware is needed at each sites. There is also less administrative overhead.
- The central computer can be very powerful: this will suit in processing-intensive applications.
- They allow a centralised approach to management. For example, a chain of shops needs to keep track of inventory in each shop and to transfer it as needed. There is little point in a shop that is running low ordering more if another branch has a surplus.

The main disadvantages of such systems are:

- Highly dependent on links to the centralised processing facility. If that machine fails or communication is disrupted then all users are affected.
- Processing speed: will decrease as more users log-on
- Lack of flexibility: local offices are dependent on suitable software and data being loaded centrally.



## Decentralised (distributed) systems

In these systems, each user has local processing power and will hold data locally.

The main advantages of such systems are:

- Resilience: if one machine breaks down, others are unaffected.
- Easy expansion: simply add another computer.
- Flexibility: local users can decide which programs and software should be installed to meet local needs.
- They are more useful where each location can operate reasonably separately from others.

The main disadvantages are:

- More difficult to control: data storage and processing are in many locations and correct access, processing and back-up of data are more difficult to enforce.
- Multiple versions of data: user might have their own version of data that should be uniform.
- Potentially higher costs: each local computer has to have sufficient processing power and each location might require an IT expert.

### 3.1. Cloud computing.

This is relatively new approach but one that is growing in popularity. There is only one copy of the software on the server within a web-based interface. Users log into the web system and their processing is then carried out on the server or a 'cloud' of servers. It appears to each user that they have a local version of the software, but what they are really seeing is the program operating in the server. As more processing is needed more cloud resources can be used and this gives users great flexibility.

Client machines can be 'thin-clients' (ie not powerful) as they do not have to store much data and software nor do they have to carry out much processing. Hardware, software and maintenance costs are greatly reduced, though the system is vulnerable to service disruption.

It can be particularly useful where a company's processing needs are very volatile. For example, a design or engineering company might need very high computing power only when rendering (ie producing detailed graphics) work. Much of the time processing needs are small. Therefore, instead of having a large computer of its own, the design company's work is hosted by a cloud-based computer (whose use is shared). That computer will be powerful enough to deal with intensive processing as needed. Also, designers can work at home, for example, on laptops. The relatively low powered laptop provides the interface but the bulk of the processing is done elsewhere.

Obviously there are risks arising from:

- Loss of communications with the cloud machine.
- Communications that are too slow.
- Confidential data is being held on a third party machine and being transmitted over public communications systems.



## 4. Risks in IT systems

IT poses particular risks to organisations' internal control and information systems and organisations must try to safeguard their data and IT systems otherwise problems can lead to their operations being severely disrupted and subsequently to lost sales, increased costs, incorrect decisions and reputational damage. Some security breaches might leave an organisation open to prosecution.

### Risks include:

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data so that they report inaccurate, misleading results. For example, in 2018 a UK bank, TSB, transferred its customers' accounts to another computer system run by Sabadell, TSB's Spanish owner. Many customers then had great difficulty accessing their accounts over the Internet or via ATM machines. In 2012 RBS, another British bank carried out a routine update of its software, but the update had been corrupted. Again, customers could not carry out transactions for up to week.
- Unauthorised access to data leading to destruction of data, improper changes to data, or inaccurate recording of transactions. In 2018, British Airways and Amazon both suffered data hacks which meant that customers' details being stolen.
- Particular risks may arise where multiple users access a common database on which everyone in the organisation relies. The data could be incorrectly amended and all users will be affected.
- Web application attacks. When you visit a website, you might simply access a static web-page which, for example, shows the name and address of the company which own the web-site. Alternatively, the web-site might load Java script (a programming language) into your browser and this is capable of carrying out processing. What you then have is a web application. For example, when you enter your credit card details into a site like Amazon, the validity of your card is checked locally because your card number has to comply with certain construction rules. Validity checking is carried out on your machine within your browser running a web application. Web application attacks might therefore try to interfere with the functionality of the web app you are running. For example, whilst checking the validity of your credit card, the altered application might now send details to the hacker.



- Malware is a term that covers all software intentionally designed to cause damage to a client computer, a server, the network or data. Malware includes:
  - ▶ Virus: a malicious program that inserts itself into another program and which then spreads by infecting other computers and data files.
  - ▶ Worm: can self replicate and which are stand-alone.
  - ▶ Trojan: a piece of software that looks harmless but which causes damage or inconvenience when run
  - ▶ Ransomware: threatens to publish the victim's data or which scrambles data until a ransom is paid.
  - ▶ Bots: derived from 'robot, this is a piece of software that carries out automated processes. For example, emails or posts on social media can be generated to give the appearance of support for particular causes.
  - ▶ Spyware. For example, a piece of malware that records you activity on the Internet and sends that information to an unauthorised third party.
  - ▶ Denial of service (DOS) attacks. Typically, the overwhelming of internet sites with demands for responses so that legitimate users are denied service.
  - ▶ Backdoors. Undocumented ways into a system so that normal log-on, password and security checks are bypassed.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties.
- Human error.
- Physical damage, such as fire or water damage.
- Industrial espionage.
- Fraud. Often easier by computer as it can be easier for the perpetrator to be disguised and small, almost trivial, amounts can be stolen many times so that the total becomes significant. IT fraud generally depends on either changing data or programs. For example, a person could commit a salary fraud either by changing their salary (ie altering data) or changing the salary program to boost net salary when a particular employee is being dealt with (a program fraud).
- Unauthorised changes to data in master files. For example, changing a selling prices or credit limit.
- Unauthorised changes to systems or programs so that they no longer operate correctly and reliably.
- Failure to make necessary changes to systems or programs to keep them up-to-date and in line with legal and business requirements.
- Potential loss of data or inability to access data as required. This could prevent, for example, the processing of internet sales.



## 5. Cyber security

In the UK, a Government organisation called the National Cyber Security Centre gives guidance on implementing the EU Directive on the security of network and information systems. It sets out a number of objectives for cyber security:

- Managing security risk
- Protecting against cyber attack
- Detecting cybersecurity events
- Minimising the impact of cyber security event

### 5.1. Managing security risk

This is high level and includes considering the organisation's attitude to risk, identifying and assessing risks, identifying essential services that must be maintained and understanding interdependencies arising from suppliers of hardware and software, and any interactions with sub-contractors.

Earlier we explained the process of risk identification, a risk register and assurance mapping. We also mentioned the severe reputational damage that can occur as a result of unethical behaviour. Digital resources are now so important and significant to many businesses that the risks that potentially arise from poor cyber security are enormous so organisations should have formal procedures in place to regularly:

- Identify potential cyber security risks. For example regularly review access control, stay aware of new threats, employ consultants to try to 'break into' the system. Analyse past problems as these will remain problems unless changes are made.
- Protect against those risks. For example, strict rules for changing passwords, anti-virus software, firewalls and staff training.
- Detect when breaches have occurred. For example, review customer reports, analyse data flows, analyse processing patterns, continually monitor network statistics.
- Respond to breached in cyber security. For example, assess the effect of any breach, start using back-up systems, reassure stakeholders, pay compensation to those affected, take measures to block any reoccurrence of the breach.

System security needs to be assessed regularly and proactively and not just as a reaction to a breach. Therefore, management should appoint a specialist committee or team whose brief is to manage cyber risks. Identified risks should be recorded in a risk register where decisions and actions will also be recorded.

It is common for organisations to also issue customers with a privacy policy statement explaining what data is held and how it is used. Some also issue a website security document. The British Airways web-page can be seen here:

[www.britishairways.com/en-gb/information/legal/website-security](http://www.britishairways.com/en-gb/information/legal/website-security)

This gives advice to customers about how to take care when on-line and also sets out the measures taken by the company. Obviously, not every detail of BA's precautions will be made public.



## 5.1. Protecting against cyber attack

- A set of comprehensive policies and processes must be developed that will protect the organisation's network and data so that essential services can be delivered.
- Identity checks and access control must be implemented so that users who have access to data are properly verified, authenticated and authorised. Think of verification as checking that a person is who they say they are (essential for issuing access credentials) and authentication is a verified person having to prove who they are each time they log-on.
- Data security. Data being stored or transmitted must be protected against unauthorised access, modification or deletion. For example, the use of passwords, encryption and back-ups will help to ensure data security.
- System security. Opportunities to attack systems (vulnerabilities) arise from:
  - flaws in the design of systems
  - features
  - user error.

For example, there should be procedures in place to ensure that software patches to counter flaws in software design are promptly implemented. Features should be kept under review and removed if not required. Users must be trained to avoid serious user error, such as leaving laptops unattended in cars.

- Resilient networks. For example, are networks well-designed with, perhaps, built-in spare capacity. Is a parallel system running at a remote location so that it can be switched to if the main system breaks down? Is the bandwidth of the network high enough to comfortably deal with peak demand?
- Staff awareness and training. Staff behaviour should be in line with the organisation's data protection policies and procedures and training is needed to ensure that this happens. It is also important to foster a security culture in which staff take an active role in maintaining and improving security.

## 5.1. Detecting cyber security events

An effective monitoring system must be in place so that security breaches and attempted security breaches are discovered. Once discovered there should be appropriate processes in place to make appropriate responses. For example, organisations can monitor the web addresses that employees are accessing. Email traffic might allow phishing attacks (where a malicious site poses as a legitimate one). Threat intelligence can be used to identify connections to IP addresses of sites known to be dangerous,

In addition to monitoring known indicators of cyber threats, organisations should also develop the capability of identifying unknown or expected threats. For example, unusual patterns of data flows around the network, user activity outside normal hours, the retrieval of a large volume of design documents.



## 5.2. Minimising the impact of cyber security events

First there should be response and recovery planning and there should be an incident response plan (for extreme incidents, sometimes known as a disaster recovery plan). Amongst other things, this plan should indicate how to assess the seriousness of the incident, how the effects of the incident might be minimised, allocate staff responsibilities and the steps they should take, how a back-up or stand by system can be switched to, how public and customer relations should be managed.

It is also important to assess how the incident occurred and what measures might prevent a repeat in the future.

## 6. IS27001

ISO27001 sets out international standards on information technology security techniques. It is a detailed document which lists 114 controls in 14 sections. We will list the 14 sections with just a few examples of the controls that might be relevant:

Control area	Sample controls
1 Information security policies	A set of policies should be defined, approved, published and communicated to staff.
2 Organisation of information security	All information security responsibilities shall be defined and allocated.  A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
3 Human resource security	Background checks/screening to be carried out on all candidates ...proportional to the classification of information to be accessed.  Disciplinary procedures in place to deal with information security breaches.
4 Asset management	IT assets identified and an inventory drawn up.  Rules for the acceptable use of IT assets to be drawn up.  Information to be classified in terms of...value and sensitivity.  Media to be disposed of securely.
5 Access control	Users shall be given access only to ...network services they have been authorised to use.  Password management systems should ensure quality passwords.
6 Cryptography	A policy for the use of cryptography to protect information shall be developed.



Control area	Sample controls
7 Physical and environmental security	<p>Secure areas shall be protected by appropriate entry controls.</p> <p>Physical protection against natural disasters, malicious attack and accidents shall be designed and applied.</p> <p>A clear desk and screen policy shall be adopted.</p>
8 Operations security	<p>The use of resources to be monitored....to ensure the required system performance.</p> <p>Detection, prevention and recovery....to protect against malware....</p>
9 Communications security	<p>Information in electronic messaging shall be appropriately protected.</p> <p>Confidentiality and non-disclosure agreements shall be documented, regularly reviewed and documented.</p>
10 System acquisition, development and maintenance	<p>Rules for the development of software shall be developed.</p> <p>Modification to software packages should be minimised and strictly controlled.</p>
11 Supplier relationships	<p>All relevant security requirements.....agrees with each supplier.</p> <p>Changes of suppliers....managed to take into account the criticality of information and the assessment of risks.</p>
12 Information security incident management	<p>Information security events to be reported to management as quickly as possible.</p> <p>Knowledge gained from investigating an incident shall be used to reduce the likelihood and effect of future incidents.</p>
13 Information security aspects of business continuity management	<p>The organisation shall establish, document and implement...procedures and controls to ensure ...continuity of information security.</p> <p>Sufficient redundancy sufficient to meet possible requirements [is surplus capacity available?].</p>
14 Compliance	<p>Appropriate procedures...compliance with legislative, regulatory and contractual requirements.</p> <p>Privacy and protection of personally identifiable information.</p>

## 7. Cyber security tools and techniques

### 7.1. Forensic analysis

'Forensic' implies that findings will be presented in a court of law or possibly some legal argument or negotiation such as the amount of compensation that can be claimed under an insurance arrangement.

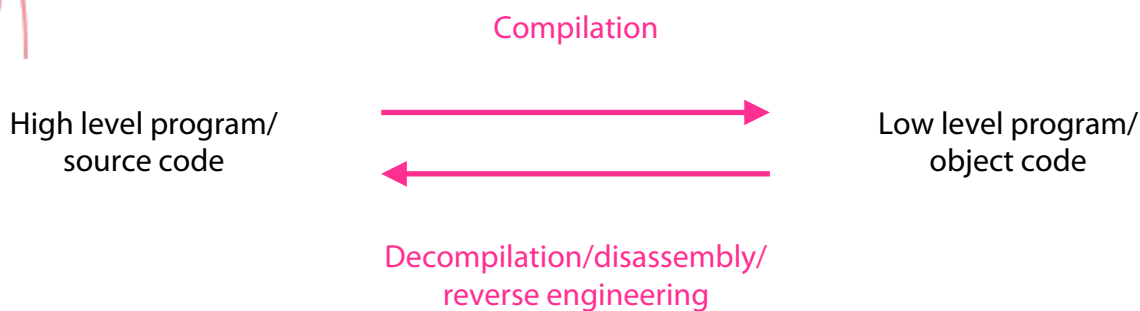
Computer forensics techniques discover, preserve and analyse information on computer systems. This involves more than just switching on the computer and searching the hard drive. Simply opening a file to read it changes it (for example date and time accessed) and therefore evidence has been changed by the action of the investigator. Therefore, when computers are seized by the police, their first action will be to remove the hard drive and to preserve the data in a completely unchanged state.

Forensic analysis will also, for example, extend to network analysis where the results can show was logged on to the system at any time, what operations they carried out, what web-sites were accessed etc.

### 7.2. Malware analysis

This aims process aims to understand what a piece of malware does and how it does it. The analysis might discover ways in which the malware can be countered.

Malware analysis often uses reverse engineering, decompilation and disassembly. What does that mean? Well, when computers are running a program, the instructions they follow have usually been converted from source code (the language they were written in) to object code (for example, a series of 1s and 0s that the computer uses ie, binary code). Therefore, malware, when it is found, will rarely be in human-readable form. The malware analyst has to take the sequences of binary code and work back to the original programming statements so that the operation of the malware can be understood.



## 7.3. Penetration testing

Penetration testing ('a pen test') is an authorised simulated cyber attack on a computer system. It is a controlled form of hacking where the hackers act on behalf of the client to probe the system for vulnerabilities. Once vulnerabilities have been found and reported, the client must take action to remedy the weaknesses and the penetration test should be repeated to see if the measures taken have been successful.

Sometimes the terms 'black hat' and 'white hat' are used to describe hackers:

- Black hat hackers: these are the baddies, illegally hacking systems for personal gain, political reasons or just for fun.
- White hat hackers: these are the good guys who try to penetrate systems on behalf of the systems owners so that system security can be improved.

Some white hat hackers may have started as black hat trackers but then decided to switch from the dark side, perhaps after a brush with the law and the opportunity to study the inside of a prison cell.

### 7.1. Software security

Software security means trying to protect software (ie programs) against malicious attacks so that the software continues to operate in the way it was designed to. For example, a program accessing a database could potentially be altered so that data was harvested, changed or deleted.

Software security can be enhanced by using good programming techniques, firewalls and intruder protection. New or amended software should be used only after strict authorisation and testing. Master copies of programs can be held off-line (so not subject to network attack) and the user copies of the software can be compared from time-to-time to the master copies to identify any changes.

Software security can be designed in layers with security set at an appropriate level for the processing being carried out and data being accessed. For example:

Tier	Description
Low	Minimum security standards. Able to withstand simple attacks
Medium	Can withstand attacks and report those attacks
High	Can withstand attacks, report attacks and make use of protective action such as locking accounts, encryption, recording the IP address of intruders.

So, a university might use the following security layers for applications

Tier	Description
Low	Academic cooperation
Medium	Email
High	HR, accounting, student records, on-line exams.



## 8. Practical controls

Controls in computer systems can be categorised as general controls and application controls.

### 8.1. General controls

These are policies and procedures that relate to the computer environment and which are therefore relevant to all applications. They support the effective functioning of application controls by helping to ensure the continued proper operation of information systems.

General IT controls that maintain the integrity of information and security of data commonly include controls over the following:

- Data centre and network operations. A data centre is a central repository of data and it is important that controls there include back-up procedures, anti-virus software and firewalls to prevent hackers gaining access. Organisations should also have disaster recovery plans in place to minimise damage caused by events such as floods, fire and terrorist activities.
- System software acquisition, change and maintenance. System software refers to operating systems, such as Windows or Apple's OS. These systems often undergo updates as problems and vulnerabilities are identified and it is important for updates to be implemented promptly.
- Application system acquisition, development, and maintenance. Applications systems are programs that carry out specific operations needed by the company – such as calculating wages and invoices and forecasting inventory usage. Just as much damage can be done by the incorrect operation of software as by entering incorrect data. For example, think of the damage that could be done if sales analyses were incorrectly calculated and presented. Management could be led to withdraw products that are, in fact, very popular. All software amendments must be carefully specified and tested before implementation.
- Access security. Physical access to file servers should be carefully controlled. This is where the company keeps its data and it is essential that this is safeguarded: data will usually endow companies with competitive advantage. Access to processing should also be restricted, typically through using log-on procedures and passwords.

### 8.1. Application controls

Application controls are manual or automated procedures that typically operate at a business process level, such as the processing of sales orders, wages and payments to suppliers.

These controls help ensure that transactions are authorised, and are completely and accurately recorded, processed and reported. Examples include:

- Edit checks of input data. For example, range tests can be applied to reject data outside an allowed range; format checks ensure that data is input in the correct format (credit card numbers should be 12 digits long; dependency checks where one piece of data implies something about another (you have probably had a travel booking rejected because you inadvertently had a return date earlier than the outward date); check digits, where a number, such as an account number, is specially constructed to comply with mathematical rules.
- Numerical sequence checks to ensure that all accountable documents have been processed.
- Drop down menus which constrain choices and ensure only allowable entries can be made.
- Batch total checks.



On-line, real time systems can pose particular risks because any number of employees could be authorised to process certain transactions. Anonymity raises the prospect of both carelessness and fraud so it is important to be able to trace all transactions to their originator. This can be done by tagging each transactions with the identity of the person responsible.

Cyber-espionage is also a growing threat. Governments, competitors and criminals attempt to steal intellectual property or information about customers and contracts. Quite obviously the theft of valuable know-how will undermine a company's competitive advantage and it is essential that for organisations to defend themselves as far as possible against these threats.

## 9. Reporting cyber risk

An organisation's key stakeholders will want to know that the organisation is taking adequate steps to manage cyber risk. Stakeholders know that cyber breaches can affect the organisation's ability to function properly, might cause confidential data to be released and might cause contamination of other systems. It is therefore important that the organisation's approach to cyber risk management is made public to stakeholders so that they gain some assurance about risk mitigation.

A possible framework for cyber risk management is as follows (CGMA Cybersecurity Tool).

- Nature of the business and operations. Naturally, many of the risks that organisations are exposed to depend on their business and operations. For example, an aircraft manufacturer will possess valuable intellectual property and there is a cyber risk that this will be stolen. On the other hand, supermarkets are less likely to have that type of data.
- Nature of the information at risk. Following on from above, organisation will list the principle types of data it stores, uses and transmits.
- Risk management programme objectives. This sets out what degree of risk mitigation the organisation wants to achieve for each item of data. For example, data showing customers credit card details needs a very high level of security. Data about wages and salaries, though personal and sensitive, is less likely to lead to losses or theft.
- Specific factors affecting cybersecurity risks. For example, a company in which each employee has a laptop which they take to clients and perhaps take home, runs specific risks relating to laptop theft and therefore theft of the data it contains. Stakeholders would expect all sensitive data on the laptops to be encrypted. Another example is where an organisation holds very sensitive data about patients medical histories. There, you would normally expect a complex password system so that hospital staff (which includes administrators) see only the data they need to carry out their jobs.
- Cyber risk governance structure. Board oversight, risk committees, procedures for identifying risks and dealing with breaches, ethical commitment, training, ensuring staff are up-to-date and properly qualified.

There follow several examples of how large company have reported cyber risks in the risk section of their annual reports



## 9.1. BAE Systems

Mandated risk policy:

Identification                      Analysis                      Evaluation                      Mitigation

## 9.2. Smiths Group plc

Risk	Potential impact	Key mitigating controls
<p><b>CYBER SECURITY</b> Cyber attacks seeking to compromise the confidentiality, integrity and availability of IT systems and the data held on them are a continuing risk. We operate in markets and product areas which are known to be of interest to cyber criminals.</p>	<ul style="list-style-type: none"> <li>– Compromised confidentiality, integrity and availability of our assets resulting from a cyber attack, impacting our ability to deliver to customers and, ultimately, financial performance and reputation.</li> <li>– Exposure to significant losses in the event of a cyber security breach relating to our security or medical products. These include not only customer losses, but also those of a potentially large class of third parties.</li> </ul>	<ul style="list-style-type: none"> <li>– Board oversight of the approach to mitigating cyber risks.</li> <li>– Proactive focus on information and cyber security risks supported by a strong governance framework.</li> <li>– Group-wide assessment of critical information assets and protection to enhance security.</li> <li>– Information Security Awareness programme.</li> <li>– Security monitoring to provide early detection of hostile activity on Smiths networks and an incident management process.</li> <li>– Partnership and monitoring arrangements in place with critical third parties, including communications service providers.</li> <li>– Risk analysis and mitigation processes relating to product cyber resilience embedded in the product lifecycle process</li> </ul>



### 9.3. IAG (international Airlines Group)

Risk context	Management and mitigation
<p>The Group could face financial loss, disruption or damage to brand reputation arising from an attack on the Group's systems by criminals, terrorists or foreign governments. If the Group does not adequately protect customer and employee data, it could breach regulation and face penalties and loss of customer trust.</p>	<p>The IAG Management Committee regularly reviews cyber risk and supports Group-wide initiatives to enhance defences and response plans.</p> <p>The Committee ensures that the Group is up to date with industry standards and addresses identified weaknesses.</p> <p>There is oversight of critical systems and suppliers to ensure that the Group understands the data it holds, that it is secure and regulations are adhered to.</p> <p>A GDPR programme was implemented across the Group in 2018 as part of its ongoing privacy programmes. During 2018, the Network and Information Systems (NIS) Directive was implemented.</p> <p>British Airways, Iberia, Vueling and Aer Lingus are all within scope of the requirements, which are being addressed as part of a broader programme of activity to continuously improve cyber defences.</p> <p>In September, British Airways reported the theft of data from its customers as a result of a criminal attack on its website. The fast-moving nature of this risk means that the Group will always retain a level of vulnerability.</p>



## 9.4. Unilever plc

Description of risk	What we are doing to manage the risk
<p><b>SYSTEMS AND INFORMATION</b> Unilever's operations are increasingly dependent on IT systems and the management of information. Increasing digital interactions with customers, suppliers and consumers place ever greater emphasis on the need for secure and reliable IT systems and infrastructure and careful management of the information that is in our possession. The cyber-attack threat of unauthorised access and misuse of sensitive information or disruption to operations continues to increase. Such an attack could inhibit our business operations in a number of ways, including disruption to sales, production and cash flows, ultimately impacting our results.</p>	<p>To reduce the impact of external cyber-attacks impacting our business we have firewalls and threat monitoring systems in place, complete with immediate response capabilities to mitigate identified threats. We also maintain a global system for the control and reporting of access to our critical IT systems. This is supported by an annual programme of testing of access controls.</p> <p>We have policies covering the protection of both business and personal information, as well as the use of IT systems and applications by our employees. Our employees are trained to understand these requirements. We also have a set of IT security standards and closely monitor their operation to protect our systems and information.</p> <p>Hardware that runs and manages core operating data is fully backed up with separate contingency systems to provide real time back-up operations should they ever be required.</p> <p>We have standardised ways of hosting information on our public websites and have systems in place to monitor compliance with appropriate privacy laws and regulations, and with our own policies.</p>



## 10. Big data

### 10.1.Introduction

There are many definition the term 'big data' but most suggest something like the following:

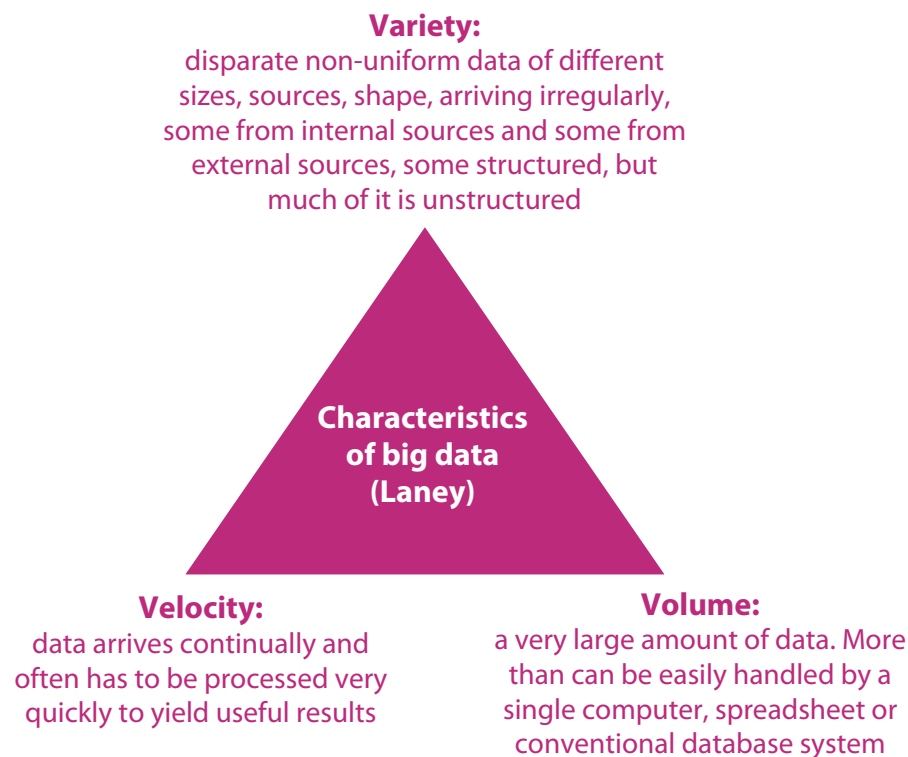
"Extremely large collections of data (data sets) that may be analysed to reveal patterns, trends, and associations, especially relating to human behaviour and interactions."

In addition, many definitions also state that the data sets are so large that conventional methods of storing and processing the data will not work.

In 2001 Doug Laney, an analyst with Gartner (a large US IT consultancy company) stated that big data has the following characteristics, known as the 3Vs:

- Volume
- Variety
- Velocity

These characteristics, and sometimes additional ones, have been generally adopted as essential qualities of big data.



The commonest fourth 'V' that is sometimes added is veracity: Is the data true? Can its accuracy be relied upon?



## 10.1.Volume

The volume of big data held by large companies such as Walmart (supermarkets), Apple and eBay is measured in multiple petabytes. What's a petabyte? It's 10<sup>15</sup> bytes (characters) of information. A typical disc on a personal computer (PC) holds 10<sup>9</sup> bytes (a gigabyte), so the big data depositories of these companies hold at least the data that could typically be held on 1 million PCs, perhaps even 10 to 20 million PCs.

These numbers probably mean little even when converted into equivalent PCs. It is more instructive to list some of the types of data that large companies will typically store.

### ● **Retailers:**

- ▶ Via loyalty cards being swiped at checkouts: details of all purchases you make, when, where, how you pay, use of coupons.
- ▶ Via websites: every product you have ever looked at, every page you have visited, every product you have ever bought. (To paraphrase a Sting song "Every click you make I'll be watching you".)
- ▶ Social media (such as Facebook and Twitter)

Friends and contacts, postings made, your location when postings are made, photographs (that can be scanned for identification), any other data you might choose to reveal to the universe.

### ● **Mobile phone companies**

Numbers you ring, texts you send (which can be automatically scanned for key words), every location your phone has ever been whilst switched on (to an accuracy of a few metres), your browsing habits. Voice mails.

### ● **Internet providers and browser providers**

Every site and every page you visit. Information about all downloads and all emails (again these are routinely scanned to provide insights into your interests). Search terms you enter.

### ● **Banking systems**

Every receipt, payment, credit card payment information (amount, date, retailer, location), location of ATM machines used.



## 10.2.Variety

Some of the variety of information can be seen from the examples listed above. In particular, the following types of information are held:

Browsing activities: sites, pages visited, membership of sites, downloads, searches

Financial transactions

- Interests
- Buying habits
- Reaction to ads on the internet or to advertising emails
- Geographical information
- Information about social and business contacts
- Text
- Numerical information
- Graphical information (such as photographs)
- Oral information (such as voice mails)
- Technical information, such as jet engine vibration and temperature analysis

**This data can be both structured and unstructured:**

**Structured data:** this data is stored within defined fields (numerical, text, date etc) often with defined lengths, within a defined record, in a file of similar records. Structured data requires a model of the types and format of business data that will be recorded and how the data will be stored, processed and accessed. This is called a data model. Designing the model defines and limits the data that can be collected and stored, and the processing that can be performed on it.

An example of structured data is found in banking systems, which record the receipts and payments from your current account: date, amount, receipt/payment, short explanations such as payee or source of the money.

Structured data is easily accessible by well-established database structured query languages.

**Unstructured data:** refers to information that does not have a pre-defined data-model. It comes in all shapes and sizes and this variety and irregularities make it difficult to store it in a way that will allow it to be analysed, searched or otherwise used. An often quoted statistic is that 80% of business data is unstructured, residing it in word processor documents, spreadsheets, PowerPoint files, audio, video, social media interactions and map data.



## 10.1.Velocity

Information must be provided quickly enough to be of use in decision making. For example, in the above store scenario, there would be little use in obtaining the price-comparison information and texting customers once they had left the store. If facial recognition is going to be used by shops and hotels, it has to be more-or less instant so that guests can be welcomed by name.

You will understand that the volume and variety conspire against the third, velocity. Methods have to be found to process huge quantities of non-uniform, awkward data in real-time.

## 10.2.Software for big data

The processing of big data is generally known as big data analytics and includes:

- **Data mining:** analysing data to identify patterns and establish relationships such as associations (where several events are connected), sequences (where one event leads to another) and correlations.
- **Predictive analytics:** a type of data mining which aims to predict future events. For example, the chance of someone being persuaded to upgrade a flight.
- **Text analytics:** scanning text such as emails and word processing documents to extract useful information. It could simply be looking for key-words that indicate an interest in a product or place.
- **Voice analytics:** as above with audio.
- **Statistical analytics:** used to identify trends, correlations and changes in behaviour.

**The analytical findings can lead to:**

- Better marketing
- Better customer service and relationship management
- Increased customer loyalty
- Increased competitive strength
- Increased operational efficiency
- The discovery of new sources of revenue.



## 10.1.Dangers of big data

Despite the examples of the use of big data in commerce, particularly for marketing and customer relationship management, there are some potential dangers and drawbacks.

- **Cost:** It is expensive to establish the hardware and analytical software needed, though these costs are continually falling.
- **Regulation:** Some countries and cultures worry about the amount of information that is being collected and have passed laws governing its collection, storage and use. Breaking a law can have serious reputational and punitive consequences.
- **Loss and theft of data:** Apart from the consequences arising from regulatory breaches as mentioned above, companies might find themselves open to civil legal action if data were stolen and individuals suffered as a consequence.
- **Incorrect data (veracity):** If the data held is incorrect or out of date incorrect conclusions are likely. Even if the data is correct, some correlations might be spurious leading to false positive results.
- **Employee monitoring:** Data collection methods allow employees to be monitored in detail every second of the day. Some companies place sensors in name badges so that employee movements and interactions at work can be monitored. The badged monitor to whom each employee talks and in what tone of voice. Stress levels can be measured from voice analysis also. Obviously, this information could be used to reduce stress levels and to facilitate better interactions but you will easily see how it could easily be used to put employees under severe pressure.



## 11. Data Protection Act implements Directive 95/46/EC

One of the important European laws concerns data protection. The Data Protection Act in the UK relates to personal data. We are not talking here about data relating to companies: we are talking about data relating to people.

### The act sets out certain principles:

- Data shall be processed fairly and lawfully.
- It can only be obtained for one or more specified and lawful purposes.
- It mustn't be excessive to what's required.
- It must be accurate and kept up-to-date.
- It mustn't be kept for longer than necessary.
- Personal data shall be processed only in accordance with the rights of data subjects. The data subject is a person about whom the data is held and that person has certain rights. For example they have a right to see the data and they have a right to insist that it's corrected. The people holding the data have to register with a government body and there they have to say what data is held, why it is held and to whom it might be supplied.
- Appropriate measures shall be taken against unauthorised and unlawful processing and also care has to be taken over the accidental loss or damage to personal data.
- Finally, personal data must not be transferred to a country or territory outside the European Economic Area unless there is similar legislation giving similar protection in that area.



## 12. Disaster planning

Many organisations are so reliant on the continued availability of IT that to be without it for even a short time can be very damaging. Of course more serious incidents could make an IT system unavailable for long times can be disastrous.

### June 2015, Computer Weekly

Royal Bank of Scotland (RBS) customers suffered at the hands of another IT problem as hundreds of thousands of payments failed to reach their accounts. About 600,000 payments including tax credits and disability living allowance did not arrive when expected.

RBS has been subject to costly IT problems in recent years. In 2012 customers were locked out of their accounts for days, as a result of a glitch in the CA-7 batch process scheduler, which froze 12 million accounts. Customers were left unable to access funds for a week or more as RBS, NatWest and Ulster Bank manually updated account balances.

RBS was fined £56m by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) as a result.

Companies should have disaster plans that will first offer some protection against problems but which will then allow the company's IT system to be up and running (at least the most vital elements of the system) as soon as possible.

Typical contents of a disaster plan are:

- Minimise physical risks; take regular backups of data
- Contingency planning: standby procedures, recovery procedures, personnel management:
  - Define responsibilities of staff members. Remember, normal working will have been disrupted.
  - Risk assessment – where is most attention needed? Where are we most vulnerable?
  - Prioritise – which elements of the system are the most vital to get back?
  - Back-ups and stand-by arrangements – if the computer is damaged, a standby machine (hardware duplication) will be able to pick up the processing. It should be located at a remote site.
  - Communication with staff and customers. A disaster can undermine confidence so good PR is essential.
- Business continuity planning. How will the business be carried on until normal service is resumed?



